



**Headquarters
United States Army Medical Department**

**Health Insurance Portability and Accountability Act (HIPAA)
Implementation Guide**

Version 2.0

**Prepared by
Office of the Director, Information Management Directorate**

October 2003

TABLE OF CONTENTS

1.0	INTRODUCTION	5
1.1	Purpose	5
1.2	Scope	5
1.3	Audience	5
1.4	Contributors	6
1.5	Comments and Suggested Improvements	6
2.0	HIPAA AT A GLANCE	7
2.1	Overview	7
2.2	Key Compliance Dates	8
2.3	Enforcement, Penalties, and Sanctions Against Workforce	9
2.4	Useful Department of Defense Resources	9
2.5	Useful Civilian Resources	11
3.0	DEPARTMENT OF DEFENSE APPROACH TO HIPAA COMPLIANCE	12
3.1	Overview	12
3.2	Military Health System	12
3.3	Army Medical Department	13
3.4	Headquarters Directorates, Executive Agencies, and Major Subordinate Commands	14
3.5	Medical Treatment Facilities and Dental Treatment Facilities	15
4.0	ELECTRONIC TRANSACTIONS AND CODE SETS	16
4.1	Overview	16
4.2	Military Health System Implementation Plan	17
4.3	Army Medical Department Implementation Plan	18
4.4	Headquarters Directorate, Executive Agency, Major Subordinate Command, Medical Treatment Facility, and Dental Treatment Facility Implementation Guidance	18
5.0	PRIVACY	19
5.1	Overview	19
5.2	Military Health System Implementation Plan	20
5.3	Army Medical Department Implementation Plan	22
5.4	Headquarters Directorate, Executive Agency, and Major Subordinate Command Implementation Guidance	24
5.5	Medical Treatment Facility and Dental Treatment Facility Implementation Guidance	25

6.0	SECURITY	28
6.1	Overview	28
6.2	Military Health System Implementation Plan.....	30
6.3	Army Medical Department Implementation Plan	31
6.4	Headquarters Directorate, Executive Agency, Major Subordinate Command, Medical Treatment Facility, and Dental Treatment Facility Implementation Guidance	35
7.0	UNIQUE HEALTH IDENTIFIERS	53
7.1	Overview	53
7.2	Military Health System Implementation Plan	53
7.3	Army Medical Department Implementation Plan	53
	APPENDICES.....	54
A	AMEDD HIPAA Implementation Memoranda.....	54
A-1	Appointment of HIPAA Focal Point and Multidisciplinary Team	54
A-2	Medical Information Security Readiness Team Training	56
A-3	Requirement for OCTAVE SM Training.....	59
A-4	Transmission of Patient Identifiable Medical Data Via Electronic Mail	61
A-5	Appointment of Privacy Officer	63
A-6	Contract Support for HIPAA Implementation	67
A-7	Documenting Acknowledgement of Military Health System (MHS) Notice of Privacy Practices (NOPP)	73
A-8	Data Call for Systems Transmitting HIPAA Electronic Transactions	77
A-9	HIPAA Training Requirements	79
A-10	Data Call to Assess HIPAA Privacy Rule Compliance	82
A-11	Compliance of MEDCOM Agreements with the HIPAA	84
A-12	Interim Forms for Authorization and Restriction of PHI	88
B	AMEDD HIPAA Overarching Integrated Project Team Charter and Member Information	91

C	AMEDD HIPAA Working Integrated Project Team Charters and Member Information	95
C-1	Transactions and Code Sets WIPT	95
C-2	Privacy WIPT	98
C-3	Security WIPT	102
LIST OF FIGURES AND TABLES		105
LIST OF ABBREVIATIONS AND ACRONYMS.....		106

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide guidance to the Army Medical Department (AMEDD) organizations for implementing and maintaining the requirements prescribed in the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191. The HIPAA has been described as one of the most challenging issues that health care organizations have faced in 30 years. Achieving HIPAA compliance requires a comprehensive and ongoing education program; substantial changes to the capabilities of core systems; and changes to the business processes within the AMEDD.

This guide offers a systems view of HIPAA implementation efforts throughout the Military Health System (MHS). It builds upon, complements, and is directly linked to the TRICARE Management Activity (TMA) HIPAA compliance framework. This is the second issue of this guide and it will be published on a quarterly or as needed basis during the HIPAA implementation process. Subsequent issues will update and augment information provided in previous issues.

1.2 Scope

This guide focuses on the Department of Defense (DoD) centralized implementation plan for the primary HIPAA Administrative Simplification rules – Electronic Transactions and Code Sets, Privacy, Security, and Unique Health Identifiers. While this guide only provides an overview of the HIPAA rules, it describes in detail how the TMA and AMEDD are implementing HIPAA and what the organizations must do to become HIPAA compliant. The information in this guide is organized for easy access to a particular HIPAA rule or organizational level implementation plan without having to read the entire document. Resources for additional information on HIPAA compliance are provided throughout the guide.

In this particular issue, the focus is on implementing the recently published Security Rule that has a compliance date of 21 April 2005. A section addressing the overall HIPAA enforcement procedures, penalties, and sanctions against the workforce has been added to this issue.

1.3 Audience

While HIPAA regulations impact many business processes and procedures across the organization, this guide is intended primarily for the AMEDD Headquarters Directorates, Executive Agencies, Major Subordinate Commands (MSCs), medical treatment facilities (MTFs) and dental treatment facilities (DTFs). Other organizations impacted by the HIPAA are encouraged to use this guide and adapt its plans to fit their individual needs. If you have organizational elements, programs, or systems that use or disclose protected health information (PHI), this guide is for you!

1.4 Contributors

This guide was developed by the AMEDD HIPAA Overarching Integrated Project Team (OIPT) under the strategic direction of the AMEDD Chief Information Officer (CIO). A list of the AMEDD HIPAA OIPT members is provided at Appendix B. The following persons were primary contributors to the accomplishment of this guide.

	Name/Title/Agency
HIPAA Program	LTC Davette Murray, Deputy CIO Office of the Assistant Chief of Staff for Information Management
	Ms. Theora Mitchell, Contractor, PEC Solutions, Inc. Office of the Assistant Chief of Staff for Information Management
	Mr. Troy Elms, Contractor, PEC Solutions, Inc. Office of the Assistant Chief of Staff for Information Management
Transactions and Code Sets	LTC Norvell Coots, Health Services Division, Office of the Assistant Chief of Staff for Health, Policy and Services
Privacy	LTC Marta Davidson, Deputy Chief, Patient Administration Division Office of the Assistant Chief of Staff for Health, Policy, and Services
	Mr. Tom Leonard, Contractor, PEC Solutions, Inc. Office of the Assistant Chief of Staff for Health Policy and Services
Security	Mr. Ross Roberts, Alternate Information Assurance Program Manager Office of the Assistant Chief of Staff for Information Management
	Mr. Chris Hastedt, Information Assurance Security Officer Office of the Assistant Chief of Staff for Information Management
	Ms. Jan Eagan, Contractor, PEC Solutions, Inc. Office of the Assistant Chief of Staff for Information Management

1.5 Comments and Suggested Improvements

Users are invited to provide comments and suggested improvements to Ms. Theora Mitchell at 210-221-8347/DSN 471 or Theora.Mitchell@amedd.army.mil.

2.0 HIPAA AT A GLANCE

2.1 Overview

Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, on 21 August 1996. The intent of the HIPAA is to restrict health insurers' ability to reject health care coverage based on pre-existing medical conditions. These insurance reform rules were expanded to include provisions for reducing health care fraud and abuse, guaranteeing security and privacy of health information, and enforcing standards for the digital transmission and storage of health information.

HIPAA comprises five titles, most of which have been in effect for several years. The exception is Title II, Subtitle F (Administrative Simplification). The Administrative Simplification provisions reduce the administrative complexity associated with the transfer of health information between organizations and will have the greatest impact on health care organizations over the next five years. The HIPAA rules and provisions are depicted below.

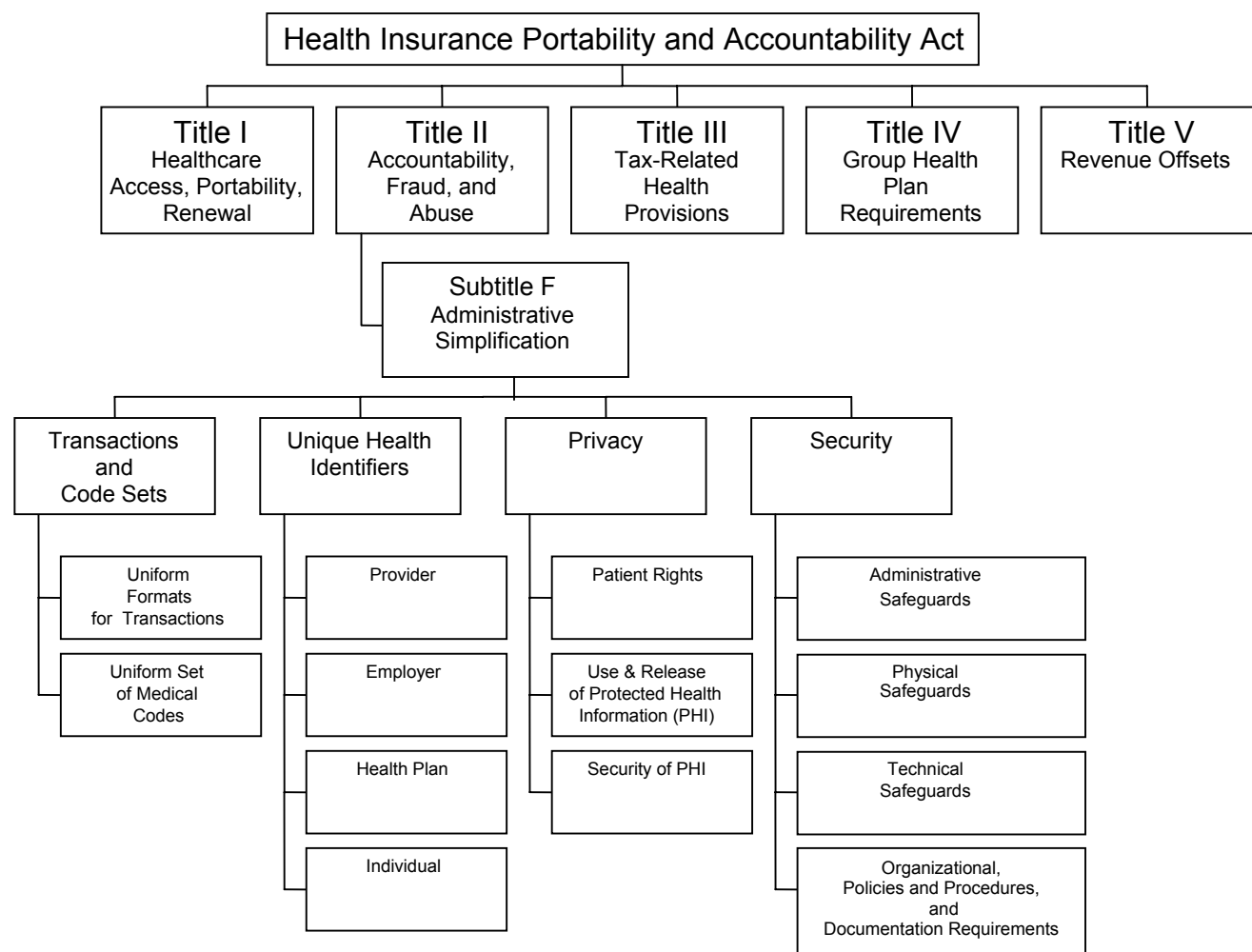


Figure 1. HIPAA Rules and Provisions.

Three of the four Administrative Simplification Rules (Electronic Transactions and Code Sets, Privacy, and Security) have been finalized and published. The fourth rule, Unique Health Identifiers, is in varying stages of completion. The Administrative Simplification Rules are discussed in Sections 4.0, 5.0, 6.0, and 7.0 of this guide.

Covered entities (CEs) must comply with the provisions of the Administrative Simplification rules. Covered entities are defined as health care providers who transmit health information in the electronic transactions covered under HIPAA; health plans; and health information clearinghouses. HIPAA rules also apply to an entity called a business associate. Business associates are individuals and companies who provide services to covered entities and require access to PHI. Covered entities are required to contract with their business associates to extend the Security and Privacy Rule requirement to protect the confidentiality of PHI.

2.2 Key Compliance Dates

The following table shows the current HIPAA compliance dates. Organizations are allowed 2 years after the effective date of the final rule to comply with the mandates. Smaller health plans are allowed an additional year.

Table 1. HIPAA Compliance Dates.

Standard		Proposed Rule	Final Rule	Compliance Date
Electronic Transactions and Code Sets		7 May 1998	17 August 2000	16 October 2003 ¹
Privacy		3 November 1999	14 April 2001 9 August 2002 ²	14 April 2003
Security		21 August 1998	21 April 2003	21 April 2005
Unique Identifiers	Employer	16 June 1998	30 July 2002	30 July 2004 ³
	Provider	7 May 1998	TBD	TBD
	Health Plan	Not Published	TBD	TBD
	Individual	Not Published	TBD	TBD
Claims Attachment Transactions		Not Published	TBD	TBD

¹ TMA submitted a compliance extension request. The request was made on behalf of TRICARE as the health plan and the MTF/DTFs as providers for the MHS. As a result of this action, TRICARE and the MHS have until 16 October 2003 to comply with the Electronic Transactions and Code Sets Rule.

² Final amendments to the Privacy Rule were published.

³ 30 July 2004 is the compliance date for large health plans (i.e., TRICARE). The date for small health plans (annual receipts of \$5M or less) is 30 July 2005.

2.3 Enforcement, Penalties, and Sanctions Against the Workforce

Although the Department of Health and Human Services (HHS) can conduct compliance reviews to determine whether covered entities are complying with the HIPAA requirements, the enforcement of HIPAA will be primarily complaint-driven. A person who believes that a covered entity is not complying with the HIPAA regulations may file a complaint with the covered entity or the HHS. The HHS intends to seek and promote voluntary compliance with the rules promulgated to carry out the HIPAA provisions. There are specific guidelines that must be followed for submitting the complaint, reviewing the complaint, and permitting access to information. On 17 April 2003, HHS published the interim final "first installment" of the HIPAA Enforcement Rule that will be published later. This interim rule establishes procedures for the imposition of civil money penalties. The final Enforcement Rule will include, among other provisions, the regulatory definition of what constitutes a violation requiring imposition of penalties and how the penalties will be determined. The HHS Office for Civil Rights (OCR) will enforce the privacy rule; the Centers for Medicare and Medicaid Services (CMS) will enforce the remaining HIPAA Administrative Simplification rules.

The HHS can impose a civil money penalty of not more than \$100 for each violation. The wrongful disclosure of Individually Identifiable Health Information (IIHI) can result in fines up to \$50,000 and imprisonment up to 1 year, or both. If the offense is committed under false pretenses, a fine of up to \$100,000 and/or imprisonment up to 5 years can be imposed. Offenses committed with intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm can result in fines up to \$250,000 and/or imprisonment up to 10 years. Civil and criminal cases will be administered by HHS and the Department of Justice, respectively.

Between 14 April and 15 June 2003, OCR reported that 637 privacy complaints were filed in a span of 62 days. Of those reports, 260 will proceed to investigation, 124 were closed without further investigation and no official decision had been made on the remaining 253 complaints. Most of the closed items reflect incidents that occurred prior to 14 April 2003. The top reasons for complaints that will be investigated include: (1) patient denied access to medical records; (2) no Notice of Privacy Practices provided to patients; and (3) inadequate safeguards in place in treatment settings.

The HIPAA also requires a covered entity to apply appropriate sanctions against members of its workforce who fail to comply with the privacy and security policies and procedures. Guidance for the application of sanctions against members of the DoD workforce is outlined in DoD Regulation 6025.18-R (DoD Health Information Privacy Regulation) and forthcoming revisions of AR 40-66 (Medical Record Administration and Health Care Documentation) and AR 40-400 (Patient Administration).

2.4 Useful Department of Defense Resources

- **TRICARE HIPAA Web Site** – <http://www.tricare.osd.mil/hipaa>. This site provides the most relevant information for implementing HIPAA within DoD organizations. The TMA uses this site to communicate HIPAA information to all MHS organizations and recommends that it be reviewed on a weekly basis to obtain the latest updates. The site has general HIPAA information, HIPAA training and compliance tools, implementation fact sheets for DoD agencies, newsletters, Frequently Asked Questions (FAQs) forums, and links to other HIPAA web sites. If

you are seeking information on the HIPAA rules or DoD HIPAA implementation policies, search this site first!

- TRICARE Standardized Materials and Research Technology (SMART) Web Site – <http://www.tricare.osd.mil/smart>. The TRICARE SMART site is the online marketing repository providing the latest TRICARE marketing news, products, template services, and guidance. The recently developed HIPAA marketing materials (posters, brochures, etc.) are available in the online TRICARE store.

- Army Knowledge Online (AKO) Web Site – <https://www.us.army.mil>. An AMEDD HIPAA file has been posted in the Army Knowledge Collaboration Center (AKCC) on the AKO Web site. This file contains the AMEDD HIPAA Implementation Guides, HIPAA Integrated Project Team meeting minutes, and a variety of other AMEDD references. To access this information, log-on to AKO and complete the following steps:

- (1) Click on “Collaborate” tab
- (2) Click on “Army Communities”
- (3) Click on “MEDCOM Community”
- (4) If you are not subscribed to “HIPAA”, click on the box next to “HIPAA”. *Subscribe Icon will highlight on top menu bar.*
- (5) Click “Subscribe”. *Subscription Request information box will open.*
- (6) Click “Finish”. *List of Subscribe Army Communities and Knowledge Centers will appear.*
- (7) Click on “HIPAA”. *You now can view the information posted in the various folders.*

- Risk Information Management Resource (RIMR) Web Site - <https://rimr.tatrc.org>. This site enables MHS to centrally manage and distribute worldwide access to a range of information sources for assessing, enhancing, studying, and archiving data about defense health information assurance. The primary audience for RIMR includes members of the Medical Information Security Readiness Team (MISRT) and other employees responsible for health information assurance. Resources include an OCTAVESM (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Information Center, reference library; technical watch; training center; and much more.

- DoD 6025.18-R (Health Information Privacy Regulation) - <http://www.dtic.mil/whs/directives/corres/html/602518r.htm>. This regulation outlines just about everything an organization needs to know and must do to implement the privacy aspects of HIPAA. All organizational entities within the Department of Defense must comply with its provisions.

2.5 Useful Civilian Resources

- Department of Health and Human Services (HHS) Web Site - <http://hhs.gov>. This is the official HHS web site for HIPAA Administrative Simplification Rules. It provides HIPAA law, history, milestones, and updates for each of the HIPAA rules. This site also has a FAQ forum and implementation guides (technical specifications for transaction standards) that can be downloaded.
- Centers for Medicare and Medicaid Services (CMS) Web Site – <http://cms.hhs.gov/hipaa>. The CMS, formerly Health Care Financing Administration (HCFA), web site provides information on the HIPAA Health Insurance Reform as well as the Administrative Simplification Rules. A HIPAA Roundtable Forum, links to recent HIPAA press releases, and the final rules in PDF format are also available on this site.
- Office for Civil Rights (OCR) Web Site – <http://hhs.gov/ocr/hipaa>. As the HHS departmental component responsible for implementing and enforcing the HIPAA Privacy regulation, this OCR site focuses on the privacy aspects of HIPAA. In addition to the updated information on the Privacy Rule, there is a Covered Entity Decision Tool that can be used to determine whether a person, business, or government agency is a covered entity and therefore subject to HIPAA rules.
- Workgroup for Electronic Data Interchange (WEDI) Web Site – <http://www.wedi.org>. The WEDI is a HIPAA designated advisor to the Secretary, HHS. In this role, WEDI established the Strategic National Implementation Process (SNIP) to help coordinate the implementation of HIPAA. This web site provides a variety of HIPAA resources to include the SNIP work products.
- American Hospital Association (AHA) Web Site – http://www.hospitalconnect.com/aha/key_issues/hipaa/index.html. While several of the HIPAA content areas are for AHA members only, there are some information resources available such as audio conferences, FAQs, fact sheets, Question and Answers Services to help hospitals respond to inquiries from patients, and numerous AHA position papers.
- Health Information Management Systems Society (HIMSS) Web Site – <http://www.himss.org/hipaasource/hipaasource.asp>. The HIMSS HIPAASource provides a listing of upcoming HIPAA events and conferences, current news, HIPAA compliance calendar, awareness information, assessment and implementation tools, hyperlinks, and FAQs. This site also provides links to the HIPAA laws and regulations.
- National HIPAA Summit Web Site - <http://www.hipaasummit.com>. The National HIPAA Summit is a leading forum on HIPAA compliance. Several 3-day HIPAA Summits are conducted yearly in various locations. The presentations from the HIPAA Summits are posed on this web site and can be accessed by clicking on “Past Summit Home” at the top of the web page.

3.0 DEPARTMENT OF DEFENSE APPROACH TO HIPAA COMPLIANCE

3.1 Overview

The DoD MHS, to include the TRICARE health plan, is both a provider of health services and a health plan or payer of health services. As such, DoD must comply with HIPAA requirements for two covered entities (providers and health plans). For purposes of the MHS, TRICARE is the health plan and the MTF/DTFs are providers. Clearinghouses that perform services (e.g., electronic billing) on behalf of the MTF/DTFs are also covered entities.

As a provider of health services, DoD provides some health services directly through the DoD MTFs, DTFs, and pharmacies and also contracts for some health services through regional networks of providers and pharmacies. In addition, DoD contracts with mail-order pharmacy providers and providers of dental services. As the TRICARE health plan, DoD performs some health plan administrative functions within DoD and contracts with Managed Care Support Contractors (MCSC) to perform some of the TRICARE health plan administrative functions. The MCSCs are business associates of the MHS.

3.2 Military Health System

The TMA, Information Management, Technology, and Reengineering Office, is tasked with planning and overseeing DoD's implementation of the HIPAA. To assist in this effort, TMA has chartered a cross-functional HIPAA Overarching Integrated Project Team (OIPT), chaired by the Chief, eHealth Requirements and Operational Architecture Division with members from the Uniformed Services and the Office of General Counsel. Several Working Integrated Project Teams (WIPTs) have been chartered under the OIPT to address specific aspects of HIPAA. The MHS HIPAA OIPT/WIPT structure is depicted below.

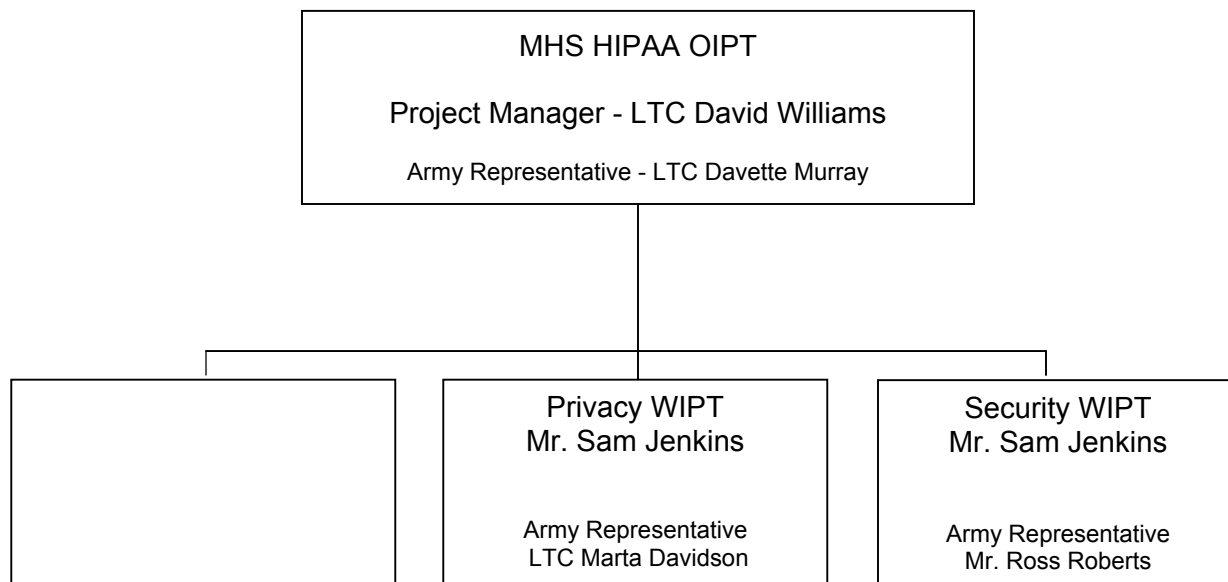


Figure 2. MHS HIPAA OIPT/WIPT Structure.

3.3 Army Medical Department

The AMEDD CIO is tasked with planning and overseeing the AMEDD's implementation of HIPAA. Similar to the MHS, Headquarters (HQ) Medical Command (MEDCOM) / Office of The Surgeon General (OTSG) has chartered a cross-functional team to assist in this effort. The AMEDD HIPAA OIPT is chaired by the Deputy CIO, with members from the functional areas and the MEDCOM MSCs. A copy of the AMEDD HIPAA OIPT charter and member information is at Appendix B. To date, three WIPTs have been chartered under the AMEDD HIPAA OIPT to address the Transactions and Code Sets, Privacy, and Security aspects of HIPAA. The WIPT Charters and member information are at Appendix C. The AMEDD HIPAA OIPT/WIPT structure is as follows:

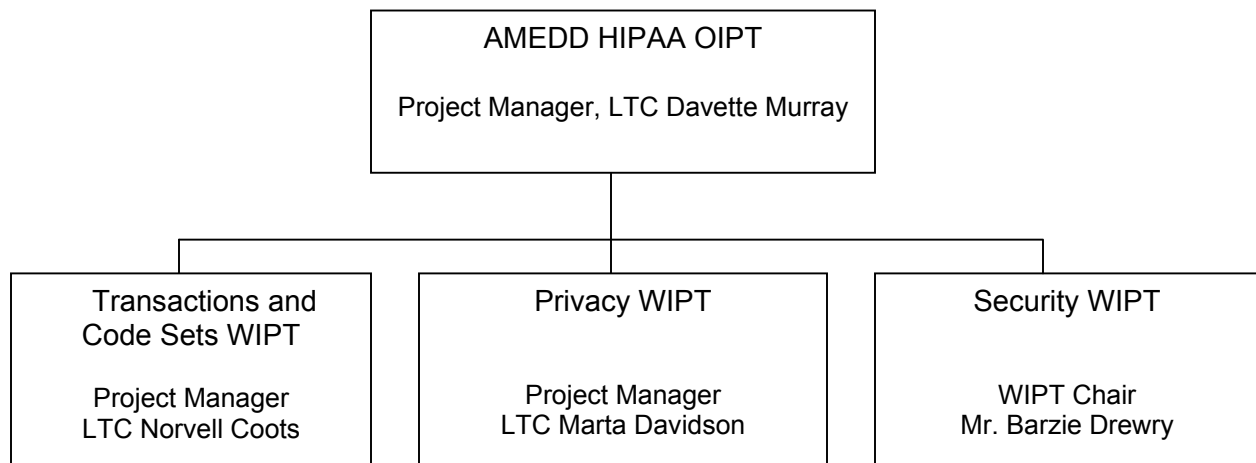


Figure 3. AMEDD HIPAA OIPT/WIPT Structure.

The primary AMEDD HIPAA points of contact are as follows:

HIPAA Program	LTC Davette Murray Davette.Murray@amedd.army.mil	(210) 221-8169/DSN 471
Transactions and Code Sets	LTC Norvell Coots Norvell.Coots@amedd.army.mil	(703) 681-0102/DSN 761
Privacy	LTC Marta Davidson Marta.Davidson@amedd.army.mil	(210) 221-6113/DSN 471
Security	Mr. Ross Roberts Ross.Roberts@amedd.army.mil	(210) 221-7869/DSN 471

3.4 Headquarters Directorates, Executive Agencies, and Major Subordinate Commands

- Headquarters Directorates, Executive Agencies, U.S. Army Medical Department Center and School (AMEDDC&S), U.S. Army Dental Command (DENCOM), U.S. Army Medical Research and Materiel Command (MRMC), and U.S. Army Center for Health Promotion and Preventive Medicine (CHPPM). These organizations will assign a HIPAA Compliance Manager and, if applicable, designate Project Managers for each of the HIPAA primary areas – Transactions and Code Sets; Privacy; and Security. The project managers will be responsible for planning and overseeing the HIPAA compliance efforts within the headquarters element and, when applicable, its subordinate units. Designation of a HIPAA Privacy Officer, Security Officer, or Medical Information Security Readiness Team (MISRT) will be at the discretion of the commander. The recommended HIPAA Implementation Team structure is depicted below in Figure 4.
- U. S. Army Regional Medical Commands (RMCs). The RMCs will assign a HIPAA Compliance Manager and designate Project Managers for each of the HIPAA primary areas - Transactions and Code Sets; Privacy; and Security, when appropriate. In addition, these organizations will also serve as the conduit between the AMEDD HIPAA OIPT/WIPT and the HIPAA Implementation Teams in their subordinate units. Designation of a RMC HIPAA Privacy Officer, Security Officer, or MISRT will be at the discretion of the commander. The recommended HIPAA Implementation Team structure is depicted below.

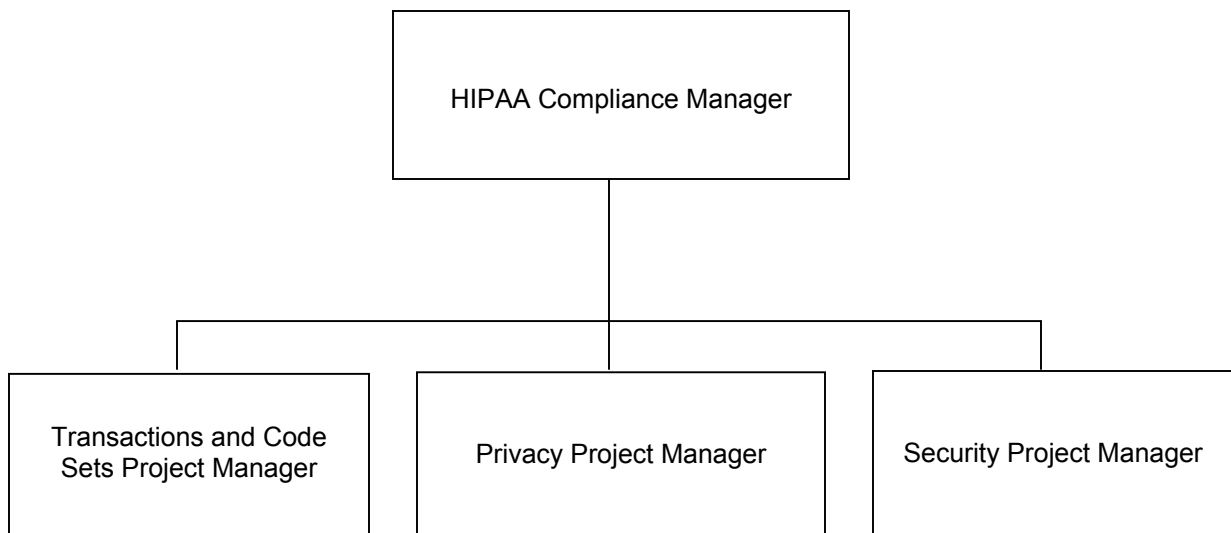


Figure 4. Headquarters Directorate, Executive Agency, and MSC HIPAA Implementation Team Structure.

3.5 Medical Treatment Facilities and Dental Treatment Facilities

The MTFs will assign a HIPAA Compliance Manager and charter a cross-functional HIPAA Implementation Team to plan and oversee the HIPAA implementation effort. In addition, the MTFs will provide support and oversee implementation activities in their medical clinics and the co-located DTFs. As directed in previous MEDCOM memoranda, the MTF commanders are required to appoint a MISRT and a HIPAA Privacy Officer. The recently published Security Rule also requires designation of a HIPAA Security official to oversee implementation of the Security Rule. The MISRT, Privacy Officer, and the Security Official should be members of the HIPAA Implementation Team. The recommended HIPAA Implementation Team structure is depicted in Figure 5.

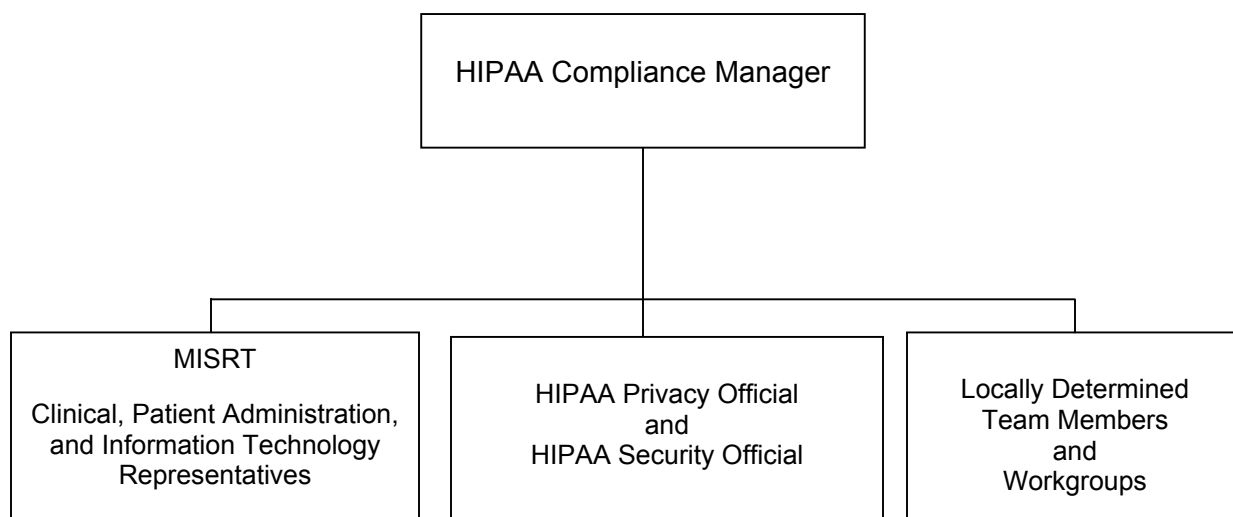


Figure 5. MTF HIPAA Implementation Team Structure.

4.0 ELECTRONIC TRANSACTIONS AND CODE SETS

4.1 Overview

The Electronic Transactions and Code Sets Rule establishes standard data content and formats for submitting electronic claims and other administrative health transactions covered under HIPAA. This part of the Administrative Simplification Compliance Act is aimed at reducing administrative costs and burdens in the health care industry. The HIPAA requires the Department of Health and Human Services (HHS) to adopt standards for financial and administrative transactions enabling health information to be exchanged electronically. The health care industry estimates that full implementation of these provisions could save as much as \$9 billion per year, while improving efficiency and enhancing the quality of health care services.

Covered entities transmitting the transactions covered under HIPAA are required to use the Accredited Standards Committee (ASC) X12N Electronic Data Interchange (EDI) uniform standards. The HIPAA mandates standard formats for the business transactions listed below. Definitions for these transactions are provided in the list of abbreviations and acronyms at end of this guide.

Claims	X12N 837
Coordination of Benefits.....	X12N 837
Claim Payment/Remittance Advice	X12N 835
Eligibility	X12N 270/271
Enrollment.....	X12N 834
Claim Status Request & Response.....	X12N 276/277
Referrals and Authorizations.....	X12N 278
Premium Payments.....	X12N 820

For most health information transactions, covered entities are required to encode health data using the uniform set of medical codes. Certain standard code sets were specified in the Transactions and Code Sets rule while others are specified in the Implementation Guides for each electronic transaction. Three such codes sets are the HIPAA Provider Taxonomy Codes, Claim Adjustment Reason Codes, and the Remittance Advice Remark Codes. The code sets listed below are already in use by DoD and will be used in the standard transactions. Definitions for the standard code sets are also provided in the list of abbreviations and acronyms at the end of this guide.

Diseases/Injuries/Procedures.....	ICD-9-CM, Vol. 1 - 3
-----------------------------------	----------------------

Physician Services.....	CPT-4
Ancillary services/procedures	HCPSC Level 1 & 2
Dental procedures.....	CDT

The HHS Centers for Medicare and Medicaid Services (CMS) is charged with enforcing the Electronic Transactions and Code Sets Rule. The HIPAA enforcement, penalties, and sanctions against the workforce are addressed in Section 2.3.

To Find Out More . . . <http://www.tricare.osd.mil/hipaa/geninfo.html>.

4.2 Military Health System Implementation Plan

The TMA HIPAA Program Office is coordinating HIPAA implementation through its HIPAA OIPT and Transactions, Code Sets, and Identifiers WIPT described in Section 3.2. The WIPT's general approach was to conduct a map/gap analysis between the Implementation guides for standard transactions and the current transactions, data elements, and code sets being used within the systems developed by TMA.

The Transactions, Code Sets and Identifiers WIPT completed the analysis of the impact of the HIPAA standard transactions on the TRICARE direct care information systems. Funding has been distributed to develop and conduct the coding and testing requirements for the information systems within the direct care program. On the purchased care side, TMA has released draft Chapter 24 to the TRICARE Operations Manual (which includes requirements for compliance with the HIPAA standard electronic transactions) to the MCSCs. The MCSCs are in the process of implementing the applicable HIPAA requirements.

The following TMA information systems send/receive HIPAA transactions and are therefore impacted by this HIPAA rule:

- Third Party Outpatient Collection System (TPOCS)
- Composite Health Care System/Ambulatory Data Module (CHCS/ADM)
- Defense Enrollment Eligibility Reporting System (DEERS)
- Claims Processing System II (CPS II)
- Pharmacy Data Transaction System (PDTS)
- MCSC Systems
- Enterprise-Wide Referral and Authorization System (EWRAS) - New System
- Executive Information/Decision Support (EI/DS)
- Patient Accounting System (PAS) - New System

The TMA HIPAA Program Office is working to ensure that when these administrative transactions are performed by the TRICARE health plan (whether directly or by contact with our business associates, such as the MCSCs), they can be performed electronically using the HIPAA standard formats. In addition, their efforts will also ensure that MHS providers (MTF/DTFs) who choose to perform one of these transactions electronically will be using a TMA system that complies with the HIPAA requirements.

The TMA tasked its system program managers to monitor and document compliance in the HIPAA BASICS™ compliance tool.

To Find Out More . . . <http://www.tricare.osd.mil/hipaa/transactions.html>.

4.3 Army Medical Department Implementation Plan

The AMEDD is coordinating implementation of the Transactions and Code Sets Rule through its HIPAA OIPT and Transactions and Code Sets WIPT described in Section 3.3. The Tertiary Care Staff Officer, Health Services Division, Health Policy and Services Directorate, is the Army representative on the MHS Transactions, Code Sets, and Identifiers WIPT and chairs the AMEDD Transactions and Code Sets WIPT. The AMEDD Transactions and Code Sets WIPT charter and member information are at Appendix C-1.

Based on the results of a recent data call, there are no AMEDD specific systems sending or receiving the transactions covered under HIPAA. The AMEDD Transactions and Code Sets WIPT will focus its efforts on writing the business rules for the new DoD systems and disseminating the related business process changes. In addition, the AMEDD will appoint functional representatives to assist TMA in evaluating technical solutions from a business process perspective. This review process will be used to assess the impact on business processes in the subordinate organizations and to validate that the TMA solution will work.

For additional information or questions regarding HIPAA Transactions and Code Sets implementation, contact LTC Norvell Coots, Norvell.Coots@amedd.army.mil or (703) 681-0102/DSN 761.

4.4 Headquarters Directorate, Executive Agency, Major Subordinate Command, Medical Treatment Facility, and Dental Treatment Facility Implementation Guidance

The AMEDD organizations are charged with implementing the business rules for new DoD systems and making the business process changes driven by the HIPAA-related changes to the DoD systems.

System developers and program managers must ensure that any systems programmed to send or receive the transactions covered under HIPAA are in compliance with the Electronic Transactions and Codes Sets Rule.

5.0 PRIVACY

5.1 Overview

The compliance date for the HIPAA Privacy Rule was 14 April 2003. This rule protects the confidentiality of patient medical data by regulating its use and disclosure by all covered entities. Individually identifiable health information (IIHI), including demographics, is protected under HIPAA. The Privacy Rule covers protected health information (PHI) stored or transmitted in any form or medium - electronic, paper, and oral. It should be noted that the HIPAA Privacy Rule is not limited to documents contained in the official medical record.

A covered entity can only use or disclose PHI for treatment, payment, and health care operations (TPO) without explicit authorization from the individual. The term “use” is defined as the internal utilization or sharing of IIHI and “disclosure” refers to the external release of IIHI. In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure.

Authorizations are required for use or disclosure of information for non-TPO purposes such as some types of research and sending marketing materials. The Privacy Rule also prescribes the elements for a valid authorization and outlines situations for which a patient's opportunity to agree or object is not required. Some examples of permitted uses or disclosures include averting serious threats to health, judicial proceedings, public health activities, and medical facility patient directories. In addition, the Privacy Rule has a military exemption clause, specific requirements for research, protection provisions for psychotherapy notes, and de-identification requirements for PHI prior to its use or disclosure.

HIPAA also increases the patient's control over his/her health information. The patient has a right to:

- A written Notice of Privacy Practices (NOPP) from health plans and providers.
- Access, inspect, and obtain a copy of PHI.
- Request an accounting of disclosures of PHI.
- Request amendment or correction of their records.
- Request restrictions on uses and disclosures of PHI.
- Receive confidential communications by alternative means/at an alternative location.
- Authorize use or disclosure of PHI for purposes other than TPO.
- Complain to the covered entity and to HHS of any violations of privacy rights.

The Privacy Rule is enforced by the Office for Civil Rights (OCR), Department of Health and Human Services. Penalties for non-compliance with the HIPAA Privacy provisions may apply to an individual violator, head of an organization, or the organization. The HIPAA enforcement, penalties, and sanctions against the workforce are addressed in Section 2.3.

To Find Out More . . . <http://www.tricare.osd.mil/hipaa/geninfo.html>.

5.2 Military Health System Implementation Plan

The DoD HIPAA Program Office is coordinating implementation through its HIPAA OIPT and the Privacy WIPT described in Section 3.2. The WIPT began holding meetings in October 2001. The TMA recognizes that implementing the HIPAA Privacy rule provisions is not a one-time project and will entail ongoing responsibilities that must be incorporated into MHS culture and business processes. To this end, TMA has completed a plethora of initiatives and purchased several tools to assist the military organizations in implementing the Privacy rule. The TMA initiatives are depicted in Table 2.

Table 2. TMA Privacy Initiatives.

Milestone	Actions
Privacy Regulation	<ul style="list-style-type: none"> Published DoD 6025.18R (DoD Health Information Privacy Regulation) prescribing uses and disclosures of PHI. Available at https://www.tricare.osd.mil/hipaa/privacy.cfm. Click on the icon for this regulation.
Privacy Officer Appointment and Job Description	<ul style="list-style-type: none"> Sent memorandum to Services directing the appointment of Privacy Officers at MTF/DTFs and attached a list of privacy officer duties. Memorandum is at Appendix A-5.
Privacy Officer Training	<ul style="list-style-type: none"> Trained over 450 MHS personnel at Privacy Officer Awareness and Training Conferences in Sep 02 and Feb 03. Training slide presentations at http://www.tricare.osd.mil/hipaa/hipaa-Privacy-Con.htm.
Workforce Training	<ul style="list-style-type: none"> Purchased web-based e-learning and tracking tool (Quick Compliance) and deployed fully operational tool in Jan 03. HIPAA training tool is available at http://hipaatraining.tricare.osd.mil.
Contract Personnel Support	Provided funds to Services for the procurement of contract personnel to support HIPAA implementation.
Marketing Materials for Privacy Initiatives	<ul style="list-style-type: none"> Developed and posted marketing materials for privacy initiatives on the TRICARE SMART Site for online procurement. Marketing materials available at http://www.tricare.osd.mil/smart.
Notice of Privacy Practices (NOPP)	<ul style="list-style-type: none"> Mailed to TRICARE beneficiaries starting Dec 02 through Mar 03. NOPP is available at http://www.tricare.osd.mil/hipaa/lang-booklets.htm. Published in several languages, large print, audio summary, and Braille.

Table 2. TMA Privacy Initiatives (Continued).

Milestone	Actions
Patient Acknowledgement of Receipt of NOPP	<ul style="list-style-type: none"> Published NOPP acknowledgement labels to be placed on outpatient medical record jacket. HIPAA labels available at http://www.tricare.osd.mil/smart. Click on "TRICARE Store" and select "All Marketing Projects" from the TRICARE Store pull down menu. Currently establishing automated process for tracking acknowledgements.
Standard Contract Language for Business Associates	<ul style="list-style-type: none"> Developed standard language clauses for Business Associate contracts/MOA/MOUs. Standard language clauses are available at http://www.tricare.osd.mil/hipaa/privacy.cfm. Click on "Privacy-Business Associate Contract Clause". Currently identifying and incorporating privacy assurance clause in existing applicable TMA (HA) level contracts, MOAs, and MOUs.
HIPAA Policy Gap Analysis	Published the gap analysis of HIPAA Privacy standards and DoD Regulations.
PHI Disclosure Authorization Forms	<p>Directed Services to develop forms IAW HIPAA requirements for use and disclosure of PHI. Two DD Forms being staffed for publication.</p> <ul style="list-style-type: none"> DD Form XXXX, XXX 2003 - Health Information Restriction Form DD Form XXXX, XXX 2003 - Health Information Disclosure Form Available at http://www.tricare.osd.mil/hipaa.
PHI Disclosure Tracking Tool	<ul style="list-style-type: none"> Interim PHI Management Tool deployed in June 2003. Final tool to be deployed in 1QFY04.
Compliance Task Documentation and Tracking Tool	<ul style="list-style-type: none"> Purchased web-based compliance management tool (HIPAA BASICS™) to track compliance tasks for all HIPAA standards. Deployed fully operational tool in Jan 03. Conducted training for interim tool via web casts. Will conduct training for final tool via web casts.
HIPAA Briefing Templates for Special Interest Groups	<ul style="list-style-type: none"> Developed HIPAA awareness briefings for non-medical DoD agents that routinely request and use PHI to include Line Leadership, Law Enforcement, Personnel, and Beneficiaries. These awareness briefings were prepared for HIPAA Privacy Officers to use and modify as required. Available at http://tricare.osd.mil/hipaa/privacy.cfm.
Monitoring and Reporting Compliance with Privacy Standards	<ul style="list-style-type: none"> Upgraded reports function of the web-based e-learning and tracking tool and developed customized reports to improve tracking of workforce training. Conducting web casts regularly to train AMEDD users on web-based tool functions. Tracking and reporting beneficiary complaints on privacy violations to MEDCOM Staff Judge Advocate (SJA) and Privacy Officer.

To Find Out More . . . <http://tricare.osd.mil/hipaa/privacy.cfm>.

5.3 Army Medical Department Implementation Plan

The AMEDD is coordinating implementation of the Privacy Rule through its HIPAA OIPT and the Privacy WIPT described in Section 3.3. The Deputy Chief, Patient Administration Division (PAD), Health Policy and Services Directorate, is the Army representative on the MHS Privacy WIPT and chairs the AMEDD Privacy WIPT. The AMEDD Privacy WIPT charter and member information are at Appendix C-2.

Members of the AMEDD Privacy WIPT were actively involved in the development and design of the TMA Privacy Rule implementation initiatives listed in Table 2. They have been and will continue to be instrumental in ensuring the AMEDD position is considered during the development and deployment phases of these initiatives. The AMEDD Privacy Rule implementation initiatives are addressed in the following table.

Table 3. AMEDD Privacy Initiatives.

Milestone	Actions
"Plain Language" Privacy Regulation	<ul style="list-style-type: none"> Contracted with Telemedicine and Advanced Technology Research Center (TATRC) to develop a "Plain Language" version of the DoD Health Information Privacy Regulation for Army organizations. Distributed in Dec 02.
Privacy Officer Appointment	Directed RMCs to Appoint Privacy Officers. <ul style="list-style-type: none"> Copy of memorandum is at Appendix A-5. Privacy Officer duties and responsibilities are at Appendix A-5.
Privacy Officer Training	Funded Army personnel to attend Privacy Officer Awareness and Training Conference in Sep 02 and Feb 03.
Workforce Education	Assisted TMA in customizing web-based training tool for AMEDD organizations, job roles, and functional groups.
Contract Personnel Support	<ul style="list-style-type: none"> Executed funds to procure HIPAA Compliance Specialists (HCS) to support HIPAA implementation in MSC/MTF/DTF. HCSs reported to RMCs, 18th MEDCOM, and designated MTFs starting in Oct 02. MEDCOM is projected to exercise option year (Sep 03-Aug 04) of contract for continued HIPAA implementation support to MSCs, MTFs, and DTFs.
Marketing Materials for Privacy Initiatives	Tracked, notified, and assisted MSCs to obtain HIPAA Privacy marketing materials for reproduction and distribution to local community.
Notice of Privacy Practices (NOPP)	Staffed NOPP and informed RMCs/MTFs of mailing progress to ensure timely preparation for receipt of patient acknowledgements.
Patient Acknowledgement of NOPP	<ul style="list-style-type: none"> Collaborated with other Services and TMA to develop NOPP acknowledgement labels. Published instructions for use of the NOPP acknowledgement labels. Memorandum available at Appendix A-7.
System of Records Notices	<ul style="list-style-type: none"> Coordinated with the Department of the Army Privacy Act and FOIA office for review and revision of applicable System of Record Notices published in the Federal Registry.

Table 3. AMEDD Privacy Initiatives (Continued).

Milestone	Actions
Standard Contract Language for Business Associates	<ul style="list-style-type: none"> • Directorate of Resource Management published policy that directs use of HIPAA standard privacy assurance clause in applicable business associate affiliations. Memorandum available at Appendix A-11. • Commander, MEDCOM HCAA, distributed instructions to all regional contract offices directing use of HIPAA standard privacy assurance clause in applicable business associate contracts.
HIPAA Policy Gap Analysis	<ul style="list-style-type: none"> • Contracted with TATRC to conduct gap analysis of HIPAA standards with published DoD regulations and Army regulations/policies. • Coordinated development of Army policy where gaps exist. • Distributed findings to MSCs for use in gap analysis of local policies.
PHI Disclosure Authorization and Restriction Forms	<ul style="list-style-type: none"> • Collaborated with other Services to develop templates of the PHI Use/ Disclosure Authorization and Restriction Forms. • Published interim guidance for implementation of PHI Use/Disclosure Authorization and Restriction Forms. Memorandum available at Appendix A-12.
Sample Privacy Policies	Developed and distributed sample policies and procedures for MTF reference and compliance with Privacy standards. Sample policies and procedures are posted on AKO in the HIPAA Knowledge Collaboration Center at https://www.us.army.mil . Instructions for accessing the HIPAA file are provided in Section 2.4 of this guide. After accessing the HIPAA file, click on "Privacy" and then on "Sample MTF Policy".
Research Policies and Procedures	Clinical Investigation Consultant published policy on HIPAA standards for research. Policy and related briefings are posted on the AKO in the HIPAA Knowledge Collaboration Center at https://www.us.army.mil . Instructions for accessing the HIPAA files are provided in Section 2.4. After accessing the HIPAA file, click on "Privacy" and then on "HIPAA and Research".
HIPAA Applications Survey for Executive Agencies and designated MSCs	<ul style="list-style-type: none"> • Contracted with TATRC to develop and publish an analysis of privacy standards as applied to the mission and activities of 33 Executive Agencies, MRMC, CHPPM, and organizational elements under the AMEDDC&S. • Preliminary survey distributed in March 03; follow-on assessments and guidance projected for Sep 03. • Survey results are posted on AKO in the HIPAA Knowledge Collaboration Center at https://www.us.army.mil. Instructions for accessing the HIPAA file are provided in Section 2.4. After accessing the HIPAA file, click on "Privacy" and then on "Executive Agent Survey".
HIPAA Briefings for Special Interest Groups	<ul style="list-style-type: none"> • Presented Privacy awareness and applications briefings to special forums such as the Family Advocacy Program; Early Development and Intervention Services; Exceptional Family Member Program; and others. • Planning additional HIPAA awareness briefings for other non-medical groups and organizations.
PHI Disclosure Tracking Tool	Coordinating with TMA to configure and test final tool for documenting and tracking PHI Disclosures.

Table 3. AMEDD Privacy Initiatives (Continued).

Milestone	Actions
Compliance Task Documentation and Tracking Tool	Assisted TMA in customizing web-base tool to facilitate compliance tasks assignment, monitoring, documentation, and reporting.
Compliance Goals and Metrics	Coordinating with MSCs and MEDCOM Directorates to establish goals and metrics to monitor AMEDD compliance with Privacy standards as part of The Surgeon General Review and Analysis program.
Support for HIPAA Privacy Inquiries	Fielding and responding to a daily average of 40 inquiries on HIPAA Privacy standards interpretation and applications.

For additional information or questions regarding HIPAA Privacy Rule implementation, contact LTC Marta Davidson, Marta.Davidson@amedd.army.mil or 210-221-6113/DSN 471

5.4 Headquarters Directorate, Executive Agency, and Major Subordinate Command Implementation Guidance

- Headquarters Directorates, Executive Agencies, AMEDDC&S, CHPPM, MRMC, and DENCOM. These organizations have a “business associate relationship” with the MTF/DTFs and must also comply with the HIPAA Privacy Rules if they have personnel, organizational elements, programs, or systems that use or disclose PHI. As such, they are charged with conducting gap analyses and developing plans to implement the applicable Privacy standards. These organizations should appoint a HIPAA Privacy Officer or a Privacy Project Manager to oversee and monitor this implementation process throughout the organization. The general tasks are outlined in Table 4. Additional guidance is provided in the DoD Health Information Privacy Regulation.
- RMCs. The RMC Headquarters elements must also comply with the Privacy Rule if they have organizational elements, programs, or systems that use or disclose PHI. In addition, the RMCs are responsible for directing, tracking, and reporting Privacy compliance milestones for their subordinate units. The RMC tasks are outlined in Table 4 and Table 5. Additional guidance is provided in the DoD Health Information Privacy Regulation.

Table 4. General Privacy Tasks for Headquarters Directorates, Executive Agencies, and MSCs.

Milestone	Tasks
Privacy Regulation	Review DoD Health Information Privacy Regulation to direct implementation activities.
Privacy Officer	Appoint a HIPAA Privacy Officer/Privacy Project Manager, if appropriate.
Privacy Officer Training	Designated staff to attend HIPAA training conducted in Sep 02 and Feb 03.

Table 4. General Privacy Tasks for Headquarters Directorates, Executive Agencies, and MSCs (Continued).

Milestone	Tasks
Workforce Training	<ul style="list-style-type: none"> • Monitor completion of Privacy Awareness Training for personnel who have the potential to use or disclosure PHI. • HIPAA training tool is available at http://hipaatraining.tricare.osd.mil.
HIPAA Policies Gap Analysis	<ul style="list-style-type: none"> • Complete gap analysis of local regulation/policies using AMEDD gap analysis findings. • Develop and revise local policies and procedures based on gap analysis findings.
PHI Risk Assessment	Map the internal and external paths of any PHI to identify and fix breaks in the chain of confidentiality. This includes all organizational elements, programs, and systems that use or disclose PHI.
Standard Privacy Assurance Language for Business Associates	Include standard HIPAA Privacy assurance language in locally established business agreements. See Memorandum at Appendix A-11.
Research Policies and Procedures	<ul style="list-style-type: none"> • Conduct gap analysis of HIPAA research requirements and local research policies. • Develop and revise local policies and procedures based on gap analysis findings and guidance published by the Clinical Investigation Consultant.
HIPAA Applications Survey for Executive Agencies and Designated MSCs	Review and apply implementation guidelines outlined in the survey about activities using PHI at U.S. Army Executive Agencies.

Table 5. Additional Privacy Tasks for RMCs.

Milestone	Tasks
Contract Personnel Support	Integrate contract HIPAA consultants into RMC/MEDCEN HIPAA program to accomplish compliance objectives, tasks, and other requirements directed by HQ MEDCOM. See Memorandum at Appendix A-6.
Compliance Task Documentation and Tracking Tool	Monitor and track MTF/DTF compliance tasks using the web-based compliance tool (HIPAA BASICS™) per MEDCOM guidance.
Compliance Goals and Metrics	Monitor and report compliance metrics as directed by HQ MEDCOM.

5.5 Medical Treatment Facility and Dental Treatment Facility Implementation Guidance

The MTF/DTFs were charged with conducting gap analyses and developing plans to implement the Privacy Rule. In accordance with the HIPAA law and OTSG guidance, MTF and/or the DTF appointed a HIPAA Privacy Officer to oversee Privacy implementation activities. On some installations, the MTF Privacy Officer also serves as the DTF Privacy Officer. The MTFs will

provide support and oversee implementation activities in their medical clinics and the co-located DTFs. The MTF/DTF Privacy tasks are outlined in the following table. Additional information is provided in the DoD Health Information Privacy Regulation.

Table 6. Privacy Tasks for MTF/DTFs.

Milestone	Tasks
Privacy Regulation	Review DoD Health Information Privacy Regulation to direct implementation activities.
Privacy Officer Appointment	Appoint a HIPAA Privacy Officer.
Privacy Officer Training	Designate staff to attend Privacy Officer training.
Contract Personnel Support	Integrate contract HIPAA consultants into MTF/DTF HIPAA program to accomplish compliance objectives tasks, and other requirements directed by HQ MEDCOM.
Workforce Education	<ul style="list-style-type: none"> • Direct all workforce members to complete training. • HIPAA training tool is available at http://hipaatraining.tricare.osd.mil. • Monitor and report completion of HIPAA Privacy Awareness Training. • Integrate privacy training requirement into the newcomer's orientation program.
Marketing Materials for Privacy Initiatives	Post marketing materials throughout the facility. Marketing materials available at http://www.tricare.osd.mil/smart . Click on "TRICARE Store" and select "All Marketing Projects" from the TRICARE Store pull down menu.
NOPP	<ul style="list-style-type: none"> • Review and familiarize staff with content of NOPP to ensure appropriate responses to patients' concerns. NOPP available at https://www.tricare.osd.mil/hipaa/lang-booklets.htm. • NOPP published in several languages, large print, audio summary, and Braille. • Establish system for managing patient inquiries.
Patient Acknowledgement of NOPP	Obtain patient acknowledgement of receipt of NOPP. Guidance published in memorandum at Appendix A-7.
Standard Privacy Assurance Language for Business Associates	Include standard HIPAA Privacy assurance language in locally established business agreements. Sample privacy assurance clause is available at Appendix A-11.
HIPAA Policies Gap Analysis	Complete gap analysis of local regulation/policies using AMEDD gap analysis findings.
Policies and Procedures	Develop local policies and procedures based on HIPAA policies gap analysis. Sample MTF policies and procedures are posted on AKO in the HIPAA Knowledge Collaboration Center at https://www.us.army.mil . Instructions for accessing the HIPAA file are provided in Section 2.4 of this guide. After accessing the HIPAA file, click on "Privacy" and then on "Sample MTF Policy".
PHI Risk Assessment	Map the internal and external path of PHI to identify and fix breaks in the chain of confidentiality.
Privacy Complaint and Inquiry Procedures	Establish mechanism for processing and documenting privacy complaints/inquiries.

Table 6. Privacy Tasks for MTF/DTFs (Continued).

Milestone	Tasks
PHI Disclosures Tracking Tool	<ul style="list-style-type: none"> • Use TMA interim disclosure tracking tool to track disclosures. • Final tool to be deployed during 1QFY04.
Confidential Communications by Alternative Means	Establish mechanism to accommodate patient requests to receive confidential communications by alternative means or at alternative locations. Sample MTF policy is posted on AKO in the HIPAA Knowledge Collaboration Center at https://www.us.army.mil . Instructions for accessing the HIPAA file are provided in Section 2.4 of this guide. After accessing the HIPAA file, click on “Privacy” and then on “Sample MTF Policy”.
Disclosure Authorization Forms	<ul style="list-style-type: none"> • Use draft DoD forms for disclosure authorizations. <ul style="list-style-type: none"> - DD Form XXXX,XXX 2003 - Health Information - Restriction Form - DD Form XXXX,XXX 2003 - Health Information - Disclosure Form • Guidance available at Appendix A -12. • Draft DD forms also available at http://tricare.osd.mil/hipaa/privacy.cfm. The links to the forms are at the bottom of the web page.
Research Policies and Procedures	<ul style="list-style-type: none"> • Conduct gap analysis of HIPAA research requirements and local research policies. • Develop and revise local policies and procedures based on gap analysis findings.
Compliance Task Documentation and Tracking Tool	Utilize DoD-purchased web-based compliance tool (HIPAA BASICS™) to assess, track, document and report progress towards compliance of the privacy standards identified in the tool.
Compliance Goals and Metrics	Monitor and report compliance metrics as directed by HQ MEDCOM.

6.0 SECURITY

6.1 Overview

The final Security Rule was published on 20 February 2003 with a compliance date of 21 April 2005. Although this rule is not enforceable until 2005, the Department of Health and Human Services (HHS) could impose penalties for security breaches based on the Privacy Rule requirement to safeguard PHI. The Security Rule is designed to ensure the confidentiality, integrity, and availability of electronic PHI. It provides protection for all electronic PHI that is maintained (data at rest) or transmitted (data in transit), not just the information in the standard HIPAA transactions. The overall goal of the Security standards is to protect data against reasonably anticipated threats or hazards and improper use or disclosure. At the heart of the rule is the necessity for a covered entity to conduct a risk assessment that evaluates its systems and processes for potential risks and vulnerabilities to the health information and to develop, implement, and maintain appropriate security measures.

The Privacy Rule and the Security Rule are closely linked. Security is what enables privacy. Once a decision has been made about the appropriate disclosures of PHI, security is the sum total of the mechanisms that can be used to make sure that PHI is not shared inappropriately. In one way, the Privacy Rule scope is wider than that of the Security Rule because the Privacy Rule protects both paper and oral PHI in addition to electronic PHI. In another way, however, the scope of the Security Rule is wider because it also protects the integrity and availability of electronic PHI. There are some overlaps between the Privacy and Security Rules so the work that has already been done for HIPAA Privacy compliance provides a head start on complying with the Security Rule. Similarities between the two rules are depicted in the table below.

Table 7. Key Similarities Between the Privacy and Security Rules.

	Privacy Rule Standard	Security Rule Standard
Compliance Official	Designate a HIPAA privacy official.	Designate a HIPAA security official.
Access Limits to PHI	Establish minimum necessary criteria for access to PHI.	Establish appropriate controls to limit access to PHI to those individuals with a need to know.
Safeguards to Protect PHI	Implement policies and procedures to protect the privacy of PHI.	Implement policies and procedures ensuring the confidentiality, integrity, and availability of electronic PHI.
Compliance Documentation	Retain HIPAA documentation for 6 years from date of creation or date last in effect, whichever is later.	Retain HIPAA documentation for 6 years from date of creation or date last in effect, whichever is later.
Workforce Training	Train all workforce members on privacy policies and procedures.	Implement training awareness program for all members of workforce, including management.
Sanctions Against the Workforce	Apply appropriate sanctions against workforce members who fail to comply with privacy policies and procedures.	Apply appropriate sanctions against workforce members who fail to comply with security policies and procedures.
Business Associate Agreements	Obtain satisfactory assurances that business associates will safeguard PHI.	Obtain satisfactory assurances that business associates will safeguard electronic PHI.

The Security standards are based on three general concepts - flexibility, scalability, and technology neutral. The flexibility and scalability allow the standards to be interpreted and implemented appropriately from the smallest provider to the large health plan. Making the standards technology neutral ensures future technology advances can be used without having to go back and realign the standards.

It should also be noted that the standards cover all aspects of security, behavioral as well as technical. In fact, many of the standards do not have a technological component at all. Organizational culture will have a greater impact on security than technology. In order to be HIPAA compliant, information security must involve all the ways that people handle and access electronic PHI. The responsibility to implement HIPAA security standards extends to all members of an organization's workforce whether they work at home or on-site.

The HHS addresses the Security Rule requirements under the following categories:

- Administrative Safeguards. This category addresses the business processes that allow access to and protect individually identifiable health information electronically maintained, transmitted, and/or received.
- Physical Safeguards. Physical safeguard provisions cover the use of administrative measures and mechanisms to control physical access to computer systems and facilities, such as workstation security and media controls. It focuses on protecting buildings, computer rooms and computer hardware from threat of fire and other natural and environmental hazards, intrusion, and physical destruction or damage by humans.
- Technical Safeguards. This category involves protecting information as it is being processed or maintained within the system (data at rest) and as it is transmitted over a communication network (data in transit).
- Organizational Requirements. The requirements for business associate contracts and other arrangements are addressed in this category.
- Policies and Procedures and Documentation Requirements. As the title implies, this category contains standards to implement reasonable and appropriate policies and procedures to comply with the Security Rule standards and meet the documentation requirements.

Each of the above five categories includes mandatory standards as well as implementation specifications that provide instructions for implementing the standards. There are 22 mandatory standards and 41 implementation specifications. Each implementation specification is listed as "required" or "addressable". A particular standard may have no separate implementation specifications, multiple required specifications, multiple addressable specifications, or the combination of the two. The required implementation specifications must be implemented to comply with the HIPAA Security Rule. An addressable implementation specification must be considered and implemented, if appropriate. And if not appropriate, the reason why and what was done in its place must be documented. Essentially, the rule requires that everything be documented. What is documented must reflect what you actually do and it must be kept current and accurate. This documentation must be maintained for 6 years from the date of its creation or the date when it was last in effect, whichever is later.

The HHS Centers for Medicare and Medicaid Services (CMS) are charged with enforcing the Security Rule. The HIPAA enforcement, penalties, and sanctions against the workforce are addressed in Section 2.3 of this guide.

For More Information on the Security Rule . . . <http://www.tricare.osd.mil/hipaa/geninfo.html>.

6.2 Military Health System Implementation Plan

The TMA HIPAA Program Office is coordinating implementation through its HIPAA OIPT and Security WIPT described in Section 3.2 of this guide. The Security WIPT has conducted training on the security risk assessment tools, completed the gap analysis of the Security rule and military regulations, and is currently formulating strategies to implement the Security Rule. The TMA Security Rule initiatives are listed in Table 8.

Table 8. TMA Security Initiatives.

Milestone	Actions
HIPAA Policy Gap Analysis	<ul style="list-style-type: none"> Contracted with TATRC to conduct gap analysis for HIPAA Security Rule, DoD policies/regulations, and Service policies/regulations. Published gap analysis findings in Apr 03.
Risk Information Management Resource (RIMR) Web Site	<ul style="list-style-type: none"> Created a web site to enable the MHS to centrally manage and provide worldwide access to a range of information sources for assessing, enhancing, studying and archiving data about defense health information assurance. Available at https://rimr.tatrc.org.
HIPAA Requirements/Military Security Initiatives Gap Analysis	<ul style="list-style-type: none"> Mapped HIPAA security requirements to existing DoD, MHS, and Service security initiatives (e.g., DITSCAP, Public Key Infrastructure (PKI), etc.) Report release date TBD.
Implementation Plan	Develop a plan of action and milestones document for monitoring HIPAA implementation within the MHS. (Lead: Army)
DoD Health Information Security Regulation	Publish DoD Health Information Security Regulation. <ul style="list-style-type: none"> Draft regulation due Jan 04. (Lead: Navy)
Audit Program	Develop audit program and define metrics. (Lead: Coast Guard and Lead Agents)
Security Officer Designation and Job Description	Publish guidance. Date TBD.
Medical Information Security Readiness Teams (MISRT)	<ul style="list-style-type: none"> Tasked Services to establish MISRT at MTFs. MISRT comprised of clinicians, patient administration, and information technology personnel. Memorandum available at Appendix A-1.

Table 8. TMA Security Initiatives (Continued).

Milestone	Actions
Security Risk Assessment Tool	Procured risk assessment tool – Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE SM). <ul style="list-style-type: none"> • Trained over 100 AMEDD personnel in past two years. • OCTAVESM Automated Tool (OAT) available for download from the OCTAVE Information Center. To access OAT, visit https://rimr.tatrc.org and click on the hyperlink in the left column “OCTAVE Information Center”. • OAT is also available on the AKO HIPAA Knowledge Collaboration Center at https://www.us.army.mil. Instructions for accessing the HIPAA Knowledge Collaboration Center are provided in Section 2.4. of this guide. After accessing the HIPAA file, click on “Security” and then on “OCTAVE Tool”.
Standard Business Associate Clause for Contracts, MOAs, and MOUs	Publish guidance. Date TBD.
Train the Workforce	Develop HIPAA Security training program along with corresponding metrics. <ul style="list-style-type: none"> • Preliminary plan is to use the same web-based tool (Quick Compliance) that was used for Privacy Rule workforce training. • Draft plan due Jan 04. (Lead: Air Force)
Compliance Tracking and Documentation	Loaded Security Rule requirements on the same web-based compliance tool (HIPAA BASICS TM) that was used for Privacy Rule compliance tracking and documentation. <ul style="list-style-type: none"> • Availability of the tool TBD.

To Find Out More . . . <http://tricare.osd.mil/hipaa/security.html>.

6.3 Army Medical Department Implementation Plan

The AMEDD is coordinating implementation of the Security Rule through the use of its HIPAA OIPT and Security WIPT described in Section 3.3 of this guide. The Chief, Plans and Policies, Office of the Assistant Chief of Staff for Information Management is the chair of the AMEDD Security WIPT. The AMEDD Security WIPT charter and member information are at Appendix C-3. Table 9 provides a synopsis of the AMEDD security initiatives.

Although the Security Rule contains both required and addressable implementation specifications, an analysis commissioned by TMA revealed that most of the addressable implementation specifications are required by DoD, MHS, Army, or AMEDD regulations. Therefore, the AMEDD organizations must implement all of the HIPAA Security Rule requirements – the required as well as the addressable implementation specifications. A comparison of the HIPAA Security Rule and the military security requirements is provided in Table 10.

Table 9. AMEDD Security Initiatives

Milestone	Actions
HIPAA Security WIPT	Established HIPAA Security WIPT. Charter and member information is at Appendix C-3.
HIPAA Implementation Plan	<ul style="list-style-type: none"> Published Version 1.0, AMEDD HIPAA Implementation Guide in Jan 03. Second issue to be published in Oct 03.
TMA Security WIPT Planning Subcommittee	Serving as lead for the TMA HIPAA planning initiatives.
DoD Health Information Security Regulation	Assist TMA in the drafting of the DoD Health Information Security Regulation.
DoD HIPAA Training Program	Assist TMA with the development of a HIPAA Security training program for the workforce.
MISRT	Tasked MTFs to establish a MISRT. Memorandum at Appendix A-1.
OCTAVE Security Risk Assessment Training	<ul style="list-style-type: none"> Directed MSCs/MTFs to send personnel (MISRT members) to OCTAVESM training sessions. Memorandum is at Appendix A-2. Sponsored OCTAVESM training sessions at 3 locations during Aug and Sep 03. To date, 154 AMEDD personnel have been trained in the OCTAVE process and tool. List of AMEDD personnel trained in the OCTAVESM process is posted on the AKO AMEDD HIPAA Collaboration Page at https://www.us.army.mil. Instructions for accessing this site are provided in Section 2.4. of this guide. After accessing the HIPAA folder, click on "Security" and then on "OCTAVE Trained Personnel".
Security Risk Assessment	<ul style="list-style-type: none"> Tasked organizations to complete and report findings of OCTAVE security risk assessment by 30 Jan 04. Details for this reporting requirement will be published separately. OCTAVESM Automated Tool (OAT) is available on the AKO HIPAA Knowledge Collaboration Center at https://www.us.army.mil. Instructions for accessing the HIPAA Knowledge Collaboration Center are provided in Section 2.4. of this guide. After accessing the HIPAA file, click on "Security" and then on "OCTAVE Tool".
Encryption of E-mails Containing PHI	Directed the use of PKI technology to encrypt e-mails containing PHI. See Appendix A-4. Updated memorandum will be published.
Encryption of Electronic PHI Being Transmitted over Communication Networks	<ul style="list-style-type: none"> Worked with TMA to provide hardware-based Virtual Private Network (VPN). Currently, there are MHS VPNs at 43 AMEDD sites. Working with the Tri-Service Infrastructure Management Program Office (TIMPO) to deploy VPNs at remaining AMEDD sites. Working with installation DOIMs to move medical data to a Virtual Local Area Network (VLAN) at non-compliant sites (per Common User Installation Transport Network (CUITN) Data Design Guide).
Validate Compliance with Security Rule	Established requirement for Commanders to verify compliance with the standards for the Administrative Safeguards in May 04 and the remainder of the standards in Nov 04. Details will be published separately.

Table 10. Comparison of HIPAA and Military Security Requirements.

Standards		Implementation Specifications	Regulatory Guidance				
			R = Required / A = Addressable				
Ref #	Administrative Safeguards		HIPAA	DoD	MHS	Army	AMEDD
1.0	Security Management Process § 164.308(a)(1)	1.1 Risk Analysis 1.2 Risk Management 1.3 Sanction Policy 1.4 Information System Activity Review	R R R R R	R R R R R	R R R R R	R R R R R	R R R R R
2.0	Assigned Security Responsibility § 164.308(a)(2)		R	R	R	R	R
3.0	Workforce Security §164.308(a)(3)	3.1 Authorization and/or Supervision 3.2 Workforce Clearance Procedure 3.3 Termination Procedures	R A A A	R R R R	R R R R	R R R R	R R R R
4.0	Information Access Management § 164.308(a)(4)	4.1 Isolating Clearinghouse Function 4.2 Access Authorization 4.3 Access Establishment and Modification	R R A A	R NA R R	R NA R R	R NA R R	R NA R R
5.0	Security Awareness and Training § 164.308(a)(5)	5.1 Security Reminders 5.2 Protection from Malicious Software 5.3 Log-in Monitoring 5.4 Password Management	R A A A A	R R TBD TBD TBD	R R R TBD R	R R R R R	R R R R R
6.0	Security Incident Procedures § 164.308(a)(6)	6.1 Response and Reporting	R	R	R	R	R
7.0	Contingency Plan § 164.308(a)(7)	7.1 Data Backup Plan 7.2 Disaster Recovery Plan 7.3 Emergency Mode Operation Plan 7.4 Testing and Revision Procedure 7.5 Applications/Data Criticality Analysis	R R R R A A	R R R R R A	R R R R R A	R R R R R R	R R R R R R
8.0	Evaluation §164.308(a)(8)		R	R	R	R	R
9.0	Business Associate Contracts and Other Arrangements § 164.308(b)(1)	9.1 Written Contract or Other Arrangement	R R	R R	R R	R R	R R

Table 10. Comparison of HIPAA and Military Security Requirements (Continued).

Standards		Implementation Specifications	Regulatory Guidance R = Required / A = Addressable				
			HIPAA	DoD	MHS	Army	AMEDD
Ref #	Physical Safeguards						
10.0	Facility Access Controls § 164.310(a)(1)	10.1 Contingency Operations	R	R	R	R	R
		10.2 Facility Security Plan	A	R	R	R	R
		10.3 Access Control/Validation Procedures	A	R	R	R	R
		10.4 Maintenance Records	A	R	R	R	R
11.0	Workstation Use § 164.310(b)		R	R	R	R	R
12.0	Workstation Security § 164.310(c)		R	R	R	R	R
13.0	Devise and Media Controls § 164.310(d)(1)	13.1 Disposal	R	R	R	R	R
		13.2 Media Re-use	R	R	R	R	R
		13.3 Accountability	A	R	R	R	R
		13.4 Data backup and Storage	A	R	R	R	R
	Technical Safeguards						
14.0	Access Control § 164.312(a)(1)	14.1 Unique User Identification	R	R	R	R	R
		14.2 Emergency Access Procedure	R	R	R	R	R
		14.3 Automatic Logoff	A	R	R	R	R
		14.4 Encryption and Decryption	A	R	R	R	R
15.0	Audit Controls § 164.312(b)		R	R	R	R	R
16.0	Integrity § 164.312(c)(1)	16.1 Mechanism to Authenticate Electronic PHI	R	R	R	R	R
			A	R	R	R	R
17.0	Person or Entity Authentication § 164.312(d)		R	R	R	R	R
18.0	Transmission Security § 164.312(e)(1)	18.1 Integrity Controls	R	R	R	R	R
		18.2 Encryption	A	R	R	R	R
			A	R	R	R	R
	Organizational Requirements						
19.0	Business Associate Contracts or Other Arrangements § 164.314(a)(1)	19.1 Business Associate Contracts	R	R	R	R	R
		19.2 Other Arrangements	R	R	R	R	R
			R	R	R	R	R
20.0	Requirements for Group Health Plans § 164.314(b)(1)		R	NA	NA	NA	NA
	Policies and Procedures and Documentation Requirements						
21.0	Policies and Procedures § 164.316(a)		R	R	R	R	R
22.0	Documentation § 164.316(b)(1)	22.1 Time Limit	R	R	R	R	R
		22.2 Availability	R	R	R	R	R
		22.3 Updates	R	R	R	R	R

6.4 Headquarters Directorate, Executive Agency, Major Subordinate Command, Medical Treatment Facility, and Dental Treatment Facility Implementation Guidance

These organizations are tasked with implementing the HIPAA security requirements. The MTF/DTFs, as covered entities, must implement all of the security standards. The administrative organizations and staff offices, however, must implement the standards if they have electronic health information systems that maintain (store) or transmit PHI. In addition, the MSCs have the responsibility to ensure their subordinate organizations comply with the HIPAA security standards. The MTFs will provide support and oversee implementation activities in their medical clinics and the co-located DTFs.

Headquarters Directorate Directors and MSC Commanders will be asked to certify compliance with the administrative safeguards standards in May 2004 and the remaining standards in November 2004. This requirement will be published under separate cover. A synopsis of the Security Rule implementation and certification timelines is provided in Table 11. The specific Security standards, tasks, and timelines are depicted in Table 12. For reference purposes, the Security standards have been mapped to the applicable Army regulations and its identification number in the HIPAA BASICS™ compliance tool. Both tables will be updated as additional guidance and regulations are published.

Table 11. Security Rule Implementation and Certification Timelines.

HIPAA Standards (22)		Target Completion Date
Category	Reference Number	
Administrative Safeguards (9)	1.0 - 4.0	30 January 2004
	5.0 (Workforce Training)	TBD
	6.0 - 9.0	30 April 2004
Compliance Certification Report due on/about 14 May 2004		
Physical Safeguards (4)	10.0 - 13.0	30 July 2004
Technical Safeguards (5)	14.0 -18.0	29 October 2004
Organizational Requirements (2)	19.0	Previously Met ¹
	20.0	Not applicable to MHS
Policies and Documentation (2)	21.0 - 22.0	Previously Met ^{2, 3}
Compliance Certification Report due on/about 12 November 2004		

¹ Standard 19.0 (Business Associate Contracts/Other Arrangements) will be met by complying with Standard 9.0 (Business Associate Contracts and Other Arrangements).

² Standard 21.0 (Policies and Procedures) will be met by complying with the standards that require the establishment of policies and procedures.

³ Standard 22.0 (Documentation) will be met when the policies are published and each standard is documented in the HIPAA BASICS™ tool.

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
		Administrative Safeguards (§ 164.308)					
1.0		Security Management Process § 164.308(a)(1)	Implement policies and procedures to prevent, detect, contain, and correct security violations.	<ul style="list-style-type: none"> Establish and implement policies and procedures to include requirements for implementation specifications 1.1 - 1.4. 	Met by Regs AR 380-19 Chap 1	107	30 Jan 04
	1.1	Risk Analysis	Conduct assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI.	<ul style="list-style-type: none"> MTFs appoint MISRT that includes a clinician, a patient administrator, and an information technologist to lead the risk assessment process. Memorandum available at Appendix A-1. Use OCTAVESM process and tool to conduct risk assessment. Available at in https://rimr.tatrc.org. MTFs will include their medical clinics and the co-located DTFs in the security risk assessment process. Risk assessment should include an inventory of the following: (1) Policies and procedures for privacy and security; (2) Information systems and the criticality/sensitivity of the information processed; (3) Business associates with whom PHI is shared; (4) Bio-medical equipment that stores PHI; (5) Employees with dial-in remote access to patient information systems; and (6) Vendors with dial-in remote access to patient information systems. 	Met by Regs AR 380-19 1-5a 2-1e	108	

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
				<ul style="list-style-type: none">Identify personnel who have been trained in the OCTAVESM process. List of personnel trained and their location is posted on the AKO AMEDD HIPAA Collaboration Page at https://www.us.army.mil. Instructions for accessing this site are provided in Section 2.4. of this guide. After accessing the HIPAA folder, click on “Security” and then on “OCTAVE Trained Personnel”.			
				<ul style="list-style-type: none">Report findings of security risk assessment to HQ MEDCOM. Guidance for this requirement will be provided under separate cover.			
	1.2	Risk Management	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the general HIPAA Security Rules.	<ul style="list-style-type: none">Use security risk assessment findings to develop/refine security policies.	Partially Met by Regs AR 380-19 1-5c and d 1-6b 2-3a(10) 3-5b(4) Chap 5	109	
				<ul style="list-style-type: none">Conduct ongoing monitoring for compliance with security policies and procedures.			
				<ul style="list-style-type: none">Establish baseline security requirements for computer systems (PCs, laptops, servers, mainframes, applications, etc).			
				<ul style="list-style-type: none">Comply with Information Assurance Vulnerability Alert (IAVA) requirements.			
				<ul style="list-style-type: none">Comply with security Certification and Accreditation (C&A) requirements for information systems and networks.Comply with requirements for Certificate of Networkiness Program.			
						Ongoing	

**Table 12. Security Tasks and Timelines for
Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.**

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
	1.3	Sanction Policy	Implement policies and procedures for applying appropriate sanctions against workforce members who fail to comply with the security policies and procedures.	<ul style="list-style-type: none"> Refer to C14.5, DoD Regulation 6025.18-R, DoD Health Information Privacy Regulation, for additional guidance. Create and maintain appropriate union agreements where applicable. 	Partially Met by Regs AR 190-16 2-2c AR 380-19 2-3a(12) 2-4g AR 40-66 2-2c and 8-9j	110	30 Jan 04
	1.4	Information System Activity Review	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<ul style="list-style-type: none"> Determine the extent and frequency of reviews based on the organization's security environment. 	Met by Regs AR 380-19 1-6d(3)(I) 2-3a(1)	111	
2.0		Assigned Security Responsibility § 164.308(a)(2)	Designate the security official who is responsible for development and implementation of the HIPAA security policies/procedures.	<ul style="list-style-type: none"> Designate the security official in writing and communicate duties and responsibilities to the workforce. TMA will publish additional guidance. Release date TBD. 	Met by Regs AR 380-19 1-4 and 1-6d	112	30 Jan 04
3.0		Workforce Security § 164.308(a)(3)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI and to prevent those workforce members who do not have access from obtaining access to electronic PHI.	<ul style="list-style-type: none"> Establish and implement policies and procedures to include requirements in implementation specifications 3.1 - 3.3. 	Partially Met by Regs AR 380-19 1-6d(3)(b) 2-2, 2-16 + 2-17	113	30 Jan 04

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
	3.1	Authorization and/or Supervision of Workforce	Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.	<ul style="list-style-type: none"> Ensure supervision of operations and maintenance personnel by an authorized, knowledgeable person. 	Partially Met by Regs AR 380-19 2-9b	114	30 Jan 04
	3.2	Workforce Clearance Procedure	Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate.	<ul style="list-style-type: none"> Establish role-based access rules for systems containing PHI. 	Partially Met by Regs AR 380-19 1-6d(3)(b) 2-16b + c	115	
	3.3	Termination Procedures	Implement procedures for terminating access to electronic PHI when employment ends.	<ul style="list-style-type: none"> Establish access privilege removal as part of exit processing and remind exiting employees of their continued confidentiality obligations. Establish mechanism for IT to be automatically notified when a user's account should be inactivated because of employee resignation or termination. Establish mechanism for automatic expiration of access for contractors, vendors, temps, residents, medical students, etc. Include such features as changing combination locks to data center, removing name from access lists, and turning in keys, tokens, or cards that allow access. Document that access to systems ended when employment ended. 	Not Met by Current Regs Partially Met by Future Reg Draft AR 25-IA	116	

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
4.0		Information Access Management § 164.308(a)(4)	Implement policies and procedures for authorizing access to electronic PHI that are consistent with applicable requirements. (Note: This refers to the Privacy Rule “minimum necessary” requirement for use/disclosure of PHI).	<ul style="list-style-type: none"> Publish and implement policies and procedures to include requirements in implementation specifications 4.2 - 4.3. 	Partially Met by Regs AR 380-19 2-3a(2) AR 40-66 2-2a and 5-21	117	30 Jan 04
	4.1	Isolating Health Care Clearinghouse Functions	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the larger organization.	<ul style="list-style-type: none"> Not Applicable to MHS. 	NA	118	NA
	4.2	Access Authorization	Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanisms.	<ul style="list-style-type: none"> Publish access control lists. Define levels of access for all personnel authorized to access health information and how access is granted and modified. 	Partially Met by Regs AR 380-19 2-3a(2)	119	30 Jan 04
	4.3	Access Establishment and Modification	Implement policies and procedures that, based on the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation transaction, program, or process.	<ul style="list-style-type: none"> Include features such as: <ul style="list-style-type: none"> System administrators have separate User IDs for their administrator duties that are different from their normal access. Process for access privileges that can be quickly changed if there is a change in the user’s role (job transfer). 	Not Met by Regs	120	

**Table 12. Security Tasks and Timelines for
Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.**

Reference Number	HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
5.0	Security Awareness and Training § 164.308(a)(5)	Implement a security awareness and training program for all members of the workforce (including management).	<ul style="list-style-type: none"> Conduct training and monitor its completion by the workforce using the MHS web-based tool - Quick Compliance. Training modules will include features listed in implementation specifications 5.1-5.4. TMA preparing security modules. Release date TBD. Guidance for refresher training will be published at a later date. 	Partially Met by Regs AR 190-16 5-3e AR 380-19 1-4c + h 2-3a(3) 2-15	121	TBD
5.1	Security Reminders	Periodic security updates.		Met by Regs AR 380-19 2-15b	122	
5.2	Protection from Malicious Software	Procedures for guarding against, detecting, and reporting malicious software.		Partially Met by Regs AR 380-19 2-15a(1) 2-27	123	
5.3	Log-in Monitoring	Procedures for monitoring log-in attempts and reporting discrepancies.		Partially Met by Regs AR 380-19 2-23e	124	
5.4	Password Management	Procedures for creating, changing, and safeguarding passwords.		Met by Regs AR 380-19 2-14	125	

**Table 12. Security Tasks and Timelines for
Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.**

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
6.0		Security Incident Procedures § 164.308(a)(6)	Implement policies and procedures to address security incidents.	<ul style="list-style-type: none"> Establish and implement policies and procedures to include implementation specification 6.1. 	Partially Met by Regs AR 190-16 1-7a and 1-9 AR 380-19 1-6d(2)(f) 1-6d(3)(h) 2-27 G-1a(6) G-2a(5)+(6)	126	30 Apr 04
	6.1	Response and Reporting	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	<ul style="list-style-type: none"> Continue to use Commander's Critical Information Requirements (CCIR) Report to notify HQ MEDCOM. Continue to comply with MEDCOM/OTSG Policy 25-02-08, Policy for Information Assurance (IA), dated 12 Mar 02. Enclosure 1 discusses IAVAs and Encl 6 provides guidance for virus prevention and reporting. 	Partially Met by Regs AR 190-16 1-7a and 1-9 AR 380-19 1-6d(2)(f) + (3)(h) 2-27 G-1a(6) G-2a(5)+(6)	127	
7.0		Contingency Plan § 164.308(a)(7)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI.	<ul style="list-style-type: none"> Establish a Continuity of Operations Plan (COOP) that includes the plans in implementation specifications 7.1 - 7.3 and complete the tasks in implementation specifications 7.4 and 7.5. 	Met by Regs AR 380-19 1-4b(1)	128	30 Apr 04

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
	7.1	Data Backup Plan	Establish (and implement procedures to create and maintain retrievable exact copies of electronic PHI.		Not Met by Current Regs Partially Met by Future Reg Draft AR 25-IA	129	
	7.2	Disaster Recovery Plan	Establish (and implement as needed) procedures to restore any loss of data.		Partially Met by Regs AR 380-19 1-4b(1) G-1b(1)(b)	130	
	7.3	Emergency Mode Operation Plan	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.		Partially Met by Regs AR 380-19 1-4(b)(l)	131	
	7.4	Testing and Revision Procedures	Implement procedures for periodic testing and revision of contingency plans.		Partially Met by Regs AR 190-16 1-5c(2)	132	
	7.5	Applications and Data Criticality Analysis	Assess the relative criticality of specific applications and data in support of other contingency plan components.		Partially Met by Regs AR 380-19 2-2	133	

**Table 12. Security Tasks and Timelines for
Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.**

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™	Completion Date
8.0		Evaluation § 164.308(a)(8)	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI, that established the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.	<ul style="list-style-type: none"> Establish and implement policy to perform these evaluations of the security safeguards to demonstrate and document their compliance with the security Rule. 	Partially Met by Regs AR 380-19 3-4	134	30 Apr 04
				<ul style="list-style-type: none"> Conduct the initial evaluation. 			30 Apr 04
				<ul style="list-style-type: none"> Conduct subsequent evaluations when there are changes in the security environment since the last evaluation. 			Ongoing
9.0		Business Associate Contracts and Other Arrangements § 164.308(b)(1)	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.	<ul style="list-style-type: none"> Identify businesses associates that create, receive, maintain or transmit electronic PHI and document assurances through a contract or other arrangements (eg., MOAs, MOUs, etc.) as required in implementation specification 9.1. 	Not Met by Regs	135	30 Apr 04
	9.1	Written Contract or Other Arrangement	Document the satisfactory assurances through a written contract or other arrangement with the business associate that meets the requirements in Standard 19.0 below.	<ul style="list-style-type: none"> Compile a list of local contracts, and MOU/MOAs (written and verbal) where contractors have access to PHI. Refer to Appendix A -11 for sample privacy assurance clauses. Clause must be modified to incorporate Security Rule requirements. TMA will publish additional guidance. Release date TBD.. 	Not Met by Regs	136	

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
		Physical Safeguards (§ 164.310)					
10.0		Facility Access Controls § 164.310(a)(1)	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	<ul style="list-style-type: none"> Establish and implement policies and procedures to include requirements in implementation specifications 10.1 - 10.4. 	Met by Regs AR 190-16 1-1 and 2-1 AR 380-19 2-10a(2), b, and f 2-11	137	30 Jul 04
	10.1	Contingency Operations	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.		Partially Met by Regs AR 190-16 1-5(2) DA PAM 25-1-1	138	
	10.2	Facility Security Plan	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.		Partially Met by Regs AR 190-16 2-1 AR 380-19 2-10a(2), b, c + f 2-11	139	
	10.3	Access Control and Validation Procedures	Implement procedures to control and validate a person's access to facilities based on their role and function, including visitor control and control of access to software programs for testing and revision.	<ul style="list-style-type: none"> Publish an authorized personnel list for physical access to the Data Center. Require workforce members wear a picture identification badge and guest badges indicate access areas as well as expiration date written in ink. 	Partially Met by Regs AR 190-16 1-5D 2-2A	140	

**Table 12. Security Tasks and Timelines for
Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.**

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
				<ul style="list-style-type: none"> Verify authorizations and clearances for system maintenance personnel prior to their access to the Data Center. 	AR 380-19 1-6d(3)(b) 2-2b(1) - (4) AR 40-66 2-2a, b, + e		
				<ul style="list-style-type: none"> Escort and monitor system maintenance personnel during the performance of their duties. Employ card swipe or proximity cards for accessing departments that are designated restricted areas due to the nature of the information they process or store. 			
	10.4	Maintenance Records	Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for e.g., hardware, walls, doors, and locks).		Not Met by Regs	141	
11.0		Workstation Use § 164.310(b)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic PHI.	<ul style="list-style-type: none"> Identify workstations (to include mobile devices) that house PHI and address the requirements in the standard. 	Not Met by Regs	142	30 Jul 04
12.0		Workstation Security § 164.310(c)	Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users.	<ul style="list-style-type: none"> Place workstations in secure location to minimize the possibility of unauthorized access to PHI. Ensure workstation monitors are positioned to keep patients and visitors from viewing the screen. 	Met by Regs AR 380-19 2-11 1-6(3)(n)		30 Jul 04

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
				<ul style="list-style-type: none"> Use privacy screens, anti-glare screens, or screen savers if unable to locate workstation in a controlled access area. 			
13.0		Device and Media Controls §164.310(d)(1)	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.	<ul style="list-style-type: none"> Publish and implement policies and procedures to include the requirements in implementation specifications in 13.1 - 13.4. 	Partially Met by Regs AR 380-19 1-4d(4)	144	30 Jul 04
	13.1	Disposal	Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.		Not Met by Current Regs Partially Met by Future Reg Draft AR 25-IA	145	
	13.2	Media Re-use	Implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.		Partially Met by Regs AR 380-19 2-20 Appendix F	146	
	13.3	Accountability	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.		Not Met by Regs	147	
	13.4	Data Backup and Storage	Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.		Not Met by Regs	148	

**Table 12. Security Tasks and Timelines for
Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.**

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
		Technical Safeguards (§ 164.312)					
14.0		Access Control § 164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights per Standard 4.0 (Information Access Management).	Establish and implement policies and procedures to include requirements for implementation specifications 14.1 - 14.4.	Met by Regs AR 380-19 2-3a(2) + (6)	149	29 Oct 04
	14.1	Unique User Identification	Assign a unique name and/or number for identifying and tracking user identity.		Met by Regs AR 380-19 2-14a	150	
	14.2	Emergency Access Procedure	Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.		Not Met by Regs	151	
	14.3	Automatic Logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.		Not Met by Current Regs Met by Future Reg Draft AR 25-IA	152	
	14.4	Encryption and Decryption	Implement a mechanism to encrypt and decrypt electronic PHI (data at rest).	<ul style="list-style-type: none"> Employ Private and Public Key technology. 	Not Met by Regs Met by Army Messages and Memorandums	153	

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
15.0		Audit controls § 164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.		Met by Regs AR 380-19 2-3a(1)	154	29 Oct 04
16.0		Integrity § 164.312(c)(1)	Implement policies and procedures to protect electronic PHI from improper alteration or destruction.	<ul style="list-style-type: none"> Establish and implement policies and procedures to include requirements in implementation specification 16.1. 	Partially Met by Regs AR 380-19 2-3a(8)	155	29 Oct 04
	16.1	Mechanism to Authenticate Electronic PHI	Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.	<ul style="list-style-type: none"> PK enable computers, applications, servers, networked systems that handle, process, or restrict access to PHI. 	Not Met by Regs	156	
17.0		Person or Entity Authentication §164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.	<ul style="list-style-type: none"> Same as above. 	Partially Met by Regs AR 380-19 2-3a(2)	157	29 Oct 04
18.0		Transmission Security §164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.	<ul style="list-style-type: none"> Establish and implement measures in implementation specifications 18.1 and 18.2. 	Met by Regs AR 380-19 4-2 4-3b + c	158	29 Oct 04
	18.1	Integrity Controls	Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.		Not Met by Current Regs Partially Met by Future Reg Draft AR 25-IA	159	

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
	18.2	Encryption	Implement a mechanism to encrypt electronic PHI whenever deemed appropriate (data in transit).	<ul style="list-style-type: none"> Ensure the medical and dental health data are being transmitted within the MHS Virtual Private Network (VPN) domain. PK enable e-mails containing PHI. 	Partially Met by Regs AR 380-19 4-2	160	
		Organizational Requirements (§ 164.314)					
19.0		Business Associate Contracts or Other Arrangements § 164.314(a)(1)	The contract or other arrangement between the covered entity and its business associate must meet the requirements in this standard's implementation specifications.		Not Met by Regs	161	29 Oct 04
	19.1	Business Associate Contracts	The contract between a covered entity and a business associate must provide that the business associate will meet the requirements stated in the Security Rule. ¹ (Note: This standard essentially tracks the similar provisions in the Privacy Rule),	<ul style="list-style-type: none"> Incorporate requirements in business associate and vendor contracts. New contracts do not have to be entered into specifically for this purpose, if existing written contracts adequately address the applicable requirements (or can be amended to do so). Sample privacy assurance clause is available at Appendix A-11. Clause must be modified to include Security Rule requirements. TMA will publish additional guidance. Release date TBD. 	Not Met by Regs	162	29 Oct 04
	19.2	Other Arrangements	When the covered entity and its business associate are both governmental entities, the covered entity is in compliance if it meets the requirements in the Security Rule. ²	<ul style="list-style-type: none"> Incorporate requirements in MOAs and MOUs with governmental entities. 	Not Met by Regs	163	29 Oct 04

Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
20.0		Requirements for Group Health Plans	Ensure the plan sponsor will reasonably and appropriately safeguard electronic PHI.	<ul style="list-style-type: none"> Not Applicable to MHS. 	NA	164, 165, 166 and 168	NA
		Policies and Procedures and Documentation Requirements (§ 164.316)					
21.0		Policies and Procedures § 164.316(a)	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.	Conduct gap analysis of local policies and procedures against policies and procedures required by the Security Rule.	Partially Met by Regs AR 380-19 Chap 1 AR 40-66 1-1b	169	29 Oct 04
22.0		Documentation § 164.316(b)(1)	Maintain policies and procedures for compliance, as well as maintaining written/electronic records of actions, activities, or assessments.	<ul style="list-style-type: none"> Establish policies and procedures to include requirements in implementation specifications 22.1 - 22.3. Use HIPAA BASICS™ web-based tool to monitor and document compliance with the Security Rule standards. 	Partially Met by Regs AR 380-19 Entire Reg	170	29 Oct 04
	22.1			<ul style="list-style-type: none"> Maintain the policies and procedures implemented in written (which may be electronic) form. Maintain a written (which may be electronic) record of any actions, activities, or assessments required by the Security Rule. 			

**Table 12. Security Tasks and Timelines for
Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs.**

Reference Number		HIPAA Security Standards and Implementation Specifications		Tasks	Army Regulation Gap Analysis	HIPAA BASICS™ Number	Target Completion Date
	22.2	Availability	Make documentation available to those persons responsible for implementation of the procedures to which the documentation pertains.		Partially Met by Regs AR 380-19 3-2e(4) 2-15	172	
	22.3	Updates	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic PHI.		Partially Met by Regs AR 380-19 3-2e(4) 2-15	173	

¹Business Associate contract must provide that the business associate will do the following:

- (1) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the covered entity;
- (2) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- (3) Report to the covered entity any security incident of which it becomes aware;
- (4) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

² The covered entity is in compliance if enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives stated in business associate contract implementation specification stated above; or other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives in the business associate implementation specification above. The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

For additional information or questions regarding HIPAA Security Rule implementation, contact Mr. Ross Roberts, Ross.Roberts@amedd.army.mil, or 210-221-7869/DSN 471.

7.0 UNIQUE HEALTH IDENTIFIERS

7.1 Overview

The Unique Health Identifier Rules require the use of standardized, numeric or alphanumeric, codes to identify an employer, health provider, health plan, or individual (patient). These codes will be used in certain electronic transactions to facilitate electronic transaction exchanges among health care companies. The rules are in various stages of completion. A description and status of these rules is provided below.

- **Unique Employer Identifier.** For HIPAA purposes, employers are defined as the sponsors of health insurance for their employee. The standard selected for the national employer identifier is the Employer Identification Number (EIN) as issued by the Internal Revenue Service (IRS). The number is the EIN that appears on an employee's IRS Form W-2, Wage and Tax Statement and is the number that will be used to identify that employer in standard electronic health care transactions. The EINs are not considered private and may be freely exchanged by employers and others. This rule was finalized and published in the Federal Register on 31 May 2002 with a compliance date of 30 July 2004.
- **Unique Health Care Provider Identifier.** A health care provider is a provider of medical or other health services as defined in section 1861(s) of the Social Security Act, and any other person or organization that furnishes, bills for, or is paid for health care services in the normal course of business. A person or organization that conducts transactions as an agent of a health care provider is also considered a provider for purposes of this rule. The standard for the unique health care provider identifier is the national provider identifier (NPI). The NPI is a 10-position numeric identifier with a check digit in the tenth position, and no embedded intelligence in the number. NPIs will be assigned by the National Provider System (NPS), a Federally-directed registry that will contain the national provider file, with certain required information about each health care provider to uniquely identify the provider and maintain contact. The Notice of Proposed Rulemaking (NPRM) for the National Provider Identifier was published on 7 May 1998. The final rule has not been published.
- **Health Plan Identifier.** The HIPAA required the establishment of a standard national health plan identifier to be used in certain electronic transactions. To date, the HHS has not yet issued a Notice of Proposed Rulemaking for this identifier. It is anticipated that when the NPRM is issued, it will be a numeric identifier and may include sub-plan identifiers to differentiate a plan's transactions processing locations, its internal transaction routing organization, etc.
- **Unique Patient Identifier.** The HIPAA also required the establishment of a standard unique individual identifier for health care purposes to be used in certain electronic transactions. A draft NPRM has been on hold pending resolution of privacy and confidentiality issues.

7.2. Military Health System Implementation Plan. TMA has not published implementation guidance for the unique employer identifier rule.

7.3. AMEDD Implementation Plan. To be determined.

To find out more . . . <http://www.tricare.osd.mil/hipaa/geninfo.html>.

APPENDIX A-1. Appointment of HIPAA Focal Point and Multidisciplinary Team.

DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL COMMAND
3050 WORTH ROAD
FORT SAM HOUSTON, TEXAS 78234-6000

REPLY TO
ATTENTION OF

21 AUG 2000

MCIM (25)

MEMORANDUM FOR

Commanders, U.S. Army Medical Command Major Subordinate Commands
Commander, 18th Medical Command, APO AP 96205-0054

SUBJECT: Health Insurance Portability and Accountability Act
(HIPAA)

1. It is imperative that the Army Medical Department (AMEDD) take aggressive action to address the HIPAA issues to ensure patient privacy and the ability to meet information assurance requirements. Medical commanders are ultimately responsible for ensuring their units are HIPAA compliant. Every effort must be made to successfully implement these changes throughout the AMEDD community. In order to prepare for HIPAA implementation, each medical treatment facility will appoint an overall HIPAA focal point. A multidisciplinary team should also be appointed to assist with the implementation process. The core members should consist of a clinical, an administrative, and an information technology representative.

2. The Military Health System Chief Information Officers are collaborating with the Telemedicine and Advanced Technology Research Center (TATRC), U.S. Army Medical Research and Materiel Command, to provide seminars about new regulations and new tools for managing risk to military health care information. You have an opportunity to send your newly appointed core members to the TATRC seminar in your region. They will learn about upcoming regulations under HIPAA and new tools for managing risks to health care information assurance. I strongly endorse this effort and expect your full cooperation.

3. See enclosure for a proposed schedule for these regional seminars. Funding for travel and per diem within the regions is available. Submit your nominations to Mr. Willie Wright, TATRC, Commercial (301) 619-7034 or electronic mail: wright@tatrc.org who will provide the fund cites.

MCIM
SUBJECT: Health Insurance Portability and Accountability Act
(HIPAA)

4. Our point of contact is LTC Charles C. Hume, Office of the
Assistant Chief of Staff for Information Management,
DSN 471-8169 or Commercial (210) 221-8169.

Encl
as



JAMES B. PEAKE
Major General, U.S. Army
Acting Commander

APPENDIX A-2. Medical Information Security Readiness Team Training.REPLY TO
ATTENTION OFDEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL COMMAND
2060 WORTH ROAD
FORT SAM HOUSTON, TEXAS 78234-8000

29 DEC 2000

MCIM (25)

MEMORANDUM FOR

Commanders, U.S. Army Medical Command Major Subordinate Commands
Commander, 18th Medical Command, APO AF 96205-0054SUBJECT: Health Insurance Portability and Accountability Act
(HIPAA) Medical Information Security Readiness Team (MISRT)
Training Seminars

1. Reference memorandum, U.S. Army Medical Command, MCIM, 21 August 2000, subject: Health Insurance Portability and Accountability Act (HIPAA).
2. Reference above, directed that each medical treatment facility appoint an overall HIPAA focal point and a multidisciplinary team to assist with the implementation process. Core team members should consist of a clinical, an administrative, and an information technology representative.
3. We are enclosing a new schedule to replace the notional schedule for the MISRT training seminars. The first five seminars are firm. The rest are continuing to be updated with firm dates and an update will be provided at a later date.
4. Funding for travel and per diem for these team members will be provided by Telemedicine and Advanced Technology Research Center (TATRC). Submit your nominations to Mr. Wright, TATRC, Commercial (301) 619-7034 or electronic mail: wright@tatrc.org who will provide the fund cites. Request you provide a copy of your MISRT nominees to our point of contact (POC) or Mr. Michael W. Jiru, Contractor, (TRW), DSN 471-8583 or Commercial (210) 221-8583.

Printed on  Recycled Paper

MCIM

SUBJECT: Health Insurance Portability and Accountability Act
(HIPAA) Medical Information Security Readiness Team (MISRT)
Training Seminars

5. Our POC is LTC Charles C. Hume, Office of the Assistant
Chief of Staff for Information Management, DSN 471-8169 or
Commercial (210) 221-8169.

FOR THE COMMANDER:

Encl
as






THOMAS J. SEMARGE
Colonel, MS
Assistant Chief of Staff for
Information Management

**MISRT Training Seminars
Schedule of Sessions**

Date	Region	Site
Friday, Jan. 26	One	Bethesda Marriott, 5151 Pooles Hill Rd, Bethesda, MD
Monday, Jan. 29	Two	Chesapeake Conference Ctr, 900 Greenbrier Circle, Chesapeake, VA
Friday, Feb. 2	Three	Raulsston Riverfront, Two Tenth St, Augusta, GA
Monday, Feb. 5	Four	Isle of Capri, 151 Bench Blvd, Biloxi, MISS
Monday, Feb 12	Six	Windom St. Anthony, 300 East Travis, San Antonio, TX
Tuesday, Mar. 6	Eleven	Madigan Army Medical Center, Seattle, WA (pending)
Wednesday, Mar. 7	Ten	Conference Center, Travis AFB, San Francisco, CA (pending)
Thursday, Mar. 8	Nine	TBD, San Diego, CA
Monday, Mar. 12	Twelve	TBD, Honolulu, HI
Wednesday, Mar. 21	Five	Wright-Patterson AFB, Dayton, OH (pending)
Wednesday, Mar. 28	Seven & Eight	TBD, Phoenix, AZ
Tuesday, Apr. 10	Thirteen	TBD

APPENDIX A-3. Requirement for OCTAVESM Training.

	DEPARTMENT OF THE ARMY HEADQUARTERS, U.S. ARMY MEDICAL COMMAND 2050 WORTH ROAD FORT SAM HOUSTON, TEXAS 78234-6000	
REPLY TO ATTENTION OF		S: 21 August 2001
MCIM {25}		17 August 2001
 MEMORANDUM FOR Commanders, U.S. Army Medical Command Regional Medical Commands		
 SUBJECT: Health Insurance Portability and Accountability Act of 1996 (HIPAA) Summit		
 1. References:		
a. Memorandum, Headquarters, U.S. Army Medical Command, MCIM, 21 August 2000, subject: Health Insurance Portability and Accountability Act (HIPAA) (Enclosure 1).		
b. Memorandum, Headquarters, U.S. Army Medical Command, MCIM, 20 December 2000, subject: Health Insurance Portability and Accountability Act (HIPAA) Medical Information Security Readiness Team (MISRT) Training Seminars (Enclosure 2).		
c. Charter, U.S. Army Medical Command (USAMEDCOM), Health Insurance Portability and Accountability Act Integrated Program Team (HIPAA IPT), July 2001 (Enclosure 3).		
d. Memorandum, OASD(HA) TMA, 14 Aug 2001, subject: Health Insurance Portability and Accountability Act of 1996 (HIPAA) Summit (Enclosure 4).		
 2. Reference 1a and b, above, requested you establish a HIPAA Point of Contact (POC). Each medical treatment facility (MTF) should establish a HIPAA POC and a multidisciplinary MISRT team to assist with the implementation process. The MISRT core team members should consist of a clinical, an administrative, and an information technology representative.		
 3. Reference 1d, above provides us an opportunity to further develop the skills of the MISRT by participating in an enhanced training course. This Summit training session is limited to one MISRT from each Army medical center. These MISRTs are expected to use the OCTAVE training and tool set from this meeting to complete the risk assessment at the medical centers they		
 <small>Printed on  Recycled Paper</small>		

MCIM

SUBJECT: Health Insurance Portability and Accountability Act of 1996 (HIPAA) Summit

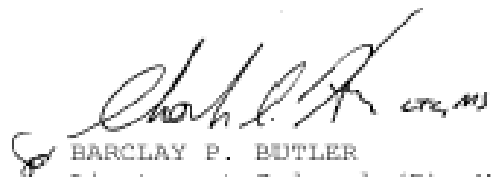
represent by 15 December 2001. The experience that this team gains, as it completes the risk assessment using the OCTAVE tool, will assist other MTFs in the RMC when they receive their follow-on training starting early 2002. Using a self-directed risk assessment will result in substantial savings to the MTF and result in a better risk assessment than one done by an outside source.

4. Please provide a current list of your HIPAA POCs and MISRT members to Mr. Michael Jiru, Contractor, TRW, not later than 31 August 2001. Since we are on a fast track to take advantage of the Summit opportunity, please provide Mr. Jiru, a list of MISRT members attending this Summit, not later than 21 August 2001. Use reference 1d, above, for registration information and the list of the original MISRT members. The attire for the conference is Class B for military and business casual for civilian attendees.

5. Our POCs are LTC Charles Hume, Office of the Assistant Chief of Staff for Information Management, DSN 471-8169 or Commercial (210) 221-8169, <mailto:Charles.Hume@amedd.army.mil> or Mr. Michael Jiru, DSN 471-8583 or Commercial (210) 221-8583, <mailto:Michael.Jiru@amedd.army.mil>


FOR THE COMMANDER:

4 Encls
as


BARCLAY P. BUTLER
Lieutenant Colonel (P), MS
Assistant Chief of Staff for
Information Management

APPENDIX A-4. Transmission of Patient Data Via Electronic Mail.

Jun-12-02	08:16am	From-	7036818903	T-047	P.001/003	F-106
-----------	---------	-------	------------	-------	-----------	-------



DEPARTMENT OF THE ARMY
OFFICE OF THE SURGEON GENERAL
5109 LEEBURN PIKE
FALLS CHURCH VA 22041-3258

REPLY TO
ATTENTION OF:

11 JUN 2002

DASG-IMD

MEMORANDUM FOR Commanders, U.S. Army MEDCOM Major Subordinate
Commands/Activities/Installations
Chiefs, Staff Offices

SUBJECT: Transmission of Patient Identifiable Medical Data Via
Electronic-Mail (E-Mail)

1. There is a recognized requirement for the U.S. Army Medical Department senior leadership to receive timely patient information associated with deployments and military operations. Such data are not envisioned to be a patient medical record or abstract, but rather patient identification, cause of injury or nature of illness, severity, prognosis, planned disposition, and the like. Although, essential for the successful conduct of deployments and military operations, such medical data must nonetheless be afforded appropriate security and protections. Transfer and release of such data must also meet the requirements set forth by the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Army Regulation 40-66, paragraph 2-4a(1).

2. Secure e-mail will be used to transmit essential patient identifiable medical data outside established reporting systems and is restricted to mission or operation-essential requirements. These e-mails will be restricted to the smallest number of users feasible. Pending final guidance as to the specific requirements associated with the exclusion the Armed Forces are granted under HIPAA, the following interim guidance is provided:

a. The Department of Defense Public Key Infrastructure (PKI) certified e-mail provides the security such medical data warrants and meets current HIPAA guidance. Accordingly, patient data transfer via e-mail will be accomplished using PKI-certified transmissions exclusively.

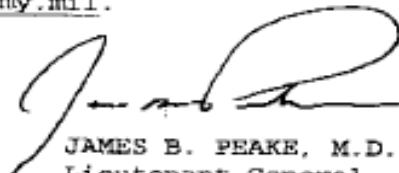
DASG-IMD

SUBJECT: Transmission of Patient Identifiable Medical Data Via Electronic-Mail (E-Mail)

b. Once received via secure, PKI-certified e-mail, patient data will be afforded the same protection and handling as that of all other medical data. The message will include a "confidentiality notice" which will address the redisclosure and destruction of disclosed information at Enclosure.



3. My point of contact is COL Barclay Butler, Assistant Chief of Staff for Information Management, DSN 761-8286 or Commercial (703) 681-8286, or email address: Barclay.Butler@otsg.amedd.army.mil.

Encl
as



JAMES B. PEAKE, M.D.
Lieutenant General
The Surgeon General

APPENDIX A-5. Appointment of Privacy Officer.

	<p>DEPARTMENT OF THE ARMY HEADQUARTERS, U.S. ARMY MEDICAL COMMAND 2060 WORTH ROAD FORT SAM HOUSTON, TEXAS 78234-6000</p>
REPLY TO ATTENTION OF	
	S: 10 September 2002 2 8 AUG 2002
MCHO-CL-P	
MEMORANDUM FOR Commanders, MEDCOM Regional Medical/Dental Commands	
SUBJECT: Appointment of Privacy Officer (PO) for Health Insurance Portability and Accountability Act (HIPAA) Compliance	
<p>1. Reference Memorandum, Office of the Assistant Secretary of Defense (Health Affairs), TRICARE Management Activity, Jun 18, 2002, subject: Request to Appoint Military Treatment Facility/Dental Treatment Facility Health Insurance Portability and Accountability Act Privacy Officer (enclosed).</p> <p>2. This memorandum is part of the continuum of HIPAA implementation requirements. The near-term HIPAA requirement is to achieve compliance with the HIPAA Privacy Rule by 14 April 2003. The Privacy Rule affects every organization and person who handles patient information and mandates the permanent appointment of POs to oversee patient health information privacy procedures.</p> <p>3. A PO must be appointed at each Regional Medical/Dental Command (RMC/RDC) and subordinate medical/dental treatment facility (MTF/DTF) in accordance with the enclosure. Where feasible, commanders should share PO resources depending on the geographic area, size, and complexity of the MTF/DTF. The enclosure includes the suggested roles and responsibilities of the PO.</p> <p>4. Please forward the names of your RMC and MTF/DTF HIPAA implementation POs no later than 10 September 2002 to LTC Marta Davidson, MEDCOM HIPAA Privacy Project Officer, DSN 471-6113; or COM (210) 221-6113; or e-mail Marta.Davidson@amedd.army.mil.</p>	
FOR THE COMMANDER:	
End	 KENNETH L. FARMER, JR. Major General Chief of Staff



TRICARE
MANAGEMENT
ACTIVITY

**OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS**

**SKYLINE FIVE, SUITE 816, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3204**

JUN 18 2002

**MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE**

SUBJECT: Request To Appoint Military Treatment Facility/Dental Treatment Facility Health Insurance Portability and Accountability Act Privacy Officer

The purpose of this letter is to request that a Privacy Officer (PO) be appointed at each Military Treatment Facility (MTF) and Dental Treatment Facility (DTF) in the Military Health System.

The Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, was enacted August 21, 1996. The purpose of the Act is to improve the portability and continuity of health insurance coverage, improve access to long term care services and coverage, and to simplify the administration of healthcare. A primary component of HIPAA administrative simplification provisions is the protection and privacy of individually identifiable health information. The HIPAA Privacy rule was signed in December 2000. Although a modification to the final rule has been proposed which will amend it, full compliance with the requirements of the HIPAA Privacy rule must still be met by April 14, 2003. The Department of Defense (DoD) HIPAA Privacy regulation, which will be completed after the modification to the final rule is completed, will describe how the Military Health System (MHS) will implement the rule.

To meet the requirements of the HIPAA Privacy rule and the DoD HIPAA Privacy regulation, a PO must be appointed at each covered entity, i.e., medical and dental facility. (Based on the size and complexity of the MTF/DTF, latitude is given to allow a PO to be responsible for more than one facility in a geographic area when smaller facilities can share resources under a mutually acceptable agreement.) The PO will be the MTF/DTF point of contact for HIPAA Privacy implementation and receive training and guidance from the respective Service HIPAA Program Office. Suggested roles and responsibilities are described in the attachment to this memorandum. It is imperative that the person selected as the MTF/DTF Privacy Officer have the requisite experience, knowledge and authority to develop, implement and monitor the privacy practices, policies and procedures throughout the facility.

HIPAA PRIVACY OFFICER ROLES AND RESPONSIBILITIES

Organizational Need/Function: The Privacy rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, requires each covered entity, i.e., medical and dental treatment facility, to appoint a Privacy Officer (PO). The PO oversees all ongoing activities related to the development, implementation, and maintenance of military treatment facility (MTF)/dental treatment facility (DTF) policies and procedures covering the access to and privacy of patient health information. The PO ensures adherence to Military Health System (MHS) policies and procedures covering these same areas. The PO also ensures MTF/DTF compliance with federal and state laws and the healthcare organization's information privacy practices, and leads initiatives to strengthen patient information privacy protections. The PO seeks to address privacy issues by balancing patient needs and the organization's requirements when making decisions related to patient health information.

Responsibilities:

Policy Implementation, Oversight, Auditing and Compliance

Develop policy and procedures for local implementation of the DoD HIPAA Privacy regulation requirements.

Maintain current knowledge of applicable federal, DoD and state privacy laws, accreditation standards, and DoD and Service regulations. Monitor advancements of emerging privacy technologies to ensure that the MTF/DTF is positioned to adapt and comply with these advancements.

- Establish and recognize best practices relative to the management of the privacy of health information.
- Serve as a liaison to the MTF/DTF Medical Information Security Readiness Team (MISRT).
- Perform initial and periodic information privacy risk assessments and conduct related ongoing compliance monitoring activities in coordination with applicable Service directives and the TMA HIPAA Office. Report findings as required.

Ensure a mechanism is in place within the MTF/DTF for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

Establish a mechanism which tracks access to protected health information, within the purview of organizational policy and as required by law, and allows qualified individuals to review or receive a report on such activity.

Education, Training and Communication

- Oversee, direct, and ensure delivery of initial privacy training and orientation to all employees, volunteers, clinical staff, business associates, and other appropriate third parties. Record results in compliance with MTF/DTF training documentation policies. Ensure annual

refresher training is conducted in order to maintain workforce awareness and to introduce any changes to privacy policies.

Initiate, facilitate and promote activities to foster information privacy awareness within the organization and related entities.

Serve as the advocate for the patient, relative to the confidentiality and privacy of health information.

MTF Integration Activities

- Understand the content of health information in its clinical, research, and business context.
- Understand the decision-making processes throughout the MTF/DTF that rely on health information. Identify and monitor the flow of information within the MTF/DTF and throughout the local healthcare network.
- Serve as privacy liaison for users of clinical and administrative systems.

Review all system-related information security plans throughout the MTF/DTF network to ensure alignment between security and privacy practices, and act as a liaison to the information systems department.

- Collaborate with other healthcare professionals to ensure appropriate security measures are in place to safeguard protected health information.

APPENDIX A-6. Contract Support for HIPAA Implementation.REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MEDICAL COMMAND
2050 WORTH ROAD
FORT SAM HOUSTON, TEXAS 78234-6013

MCHO-CL-P

21 October 2002

MEMORANDUM FOR

COMMANDERS, MEDCOM MAJOR SUBORDINATE COMMANDS
COMMANDER, 18TH MEDCOM, APO AP 96205-0054

SUBJECT: Support for Health Insurance Portability and Accountability Act (HIPAA)
Implementation

1. This memorandum is part of the continuum of HIPAA implementation requirements. The amendment to the final Privacy Rule released in August 2002 is the last change expected prior to the mandatory date of compliance, 14 April 2003. All medical treatment facilities (MTFs) and dental treatment facilities (DTFs) are required to be compliant with the HIPAA privacy standards by this date.

2. To assist MTF/DTF commanders with HIPAA implementation activities, the MEDCOM contracted on-site HIPAA consultation support. The HIPAA consultants are projected to arrive at each regional medical command by 28 October 2002. Commanders are encouraged to integrate the consultants in their implementation programs to assist with HIPAA compliance requirements.

3. The milestones for the Privacy standards are outlined in the enclosure. Along with the arrival of the HIPAA consultants, the enclosed guidelines will help commanders reach compliance on time.

4. My point of contact is LTC Marta Davidson, MEDCOM HIPAA Privacy Project Officer, (210) 221-6113/ DSN 471-6113, or e-mail Marta.Davidson@amedd.army.mil.

FOR THE COMMANDER:

Encl


KENNETH L. FARMER, JR.
Major General
Chief of Staff

IMPLEMENTING GUIDANCE HIPAA PRIVACY RULE

Preface

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provisions is not a one-time project and will entail ongoing responsibilities that must be incorporated into the Military Health System (MHS) culture and business processes. With that focus, tasked HIPAA project teams collaborated in several initiatives to assist the military treatment facilities in implementing the Privacy Rule.

Overview

The HIPAA Privacy provisions protect the confidentiality of patient medical data by regulating its use and disclosure by all covered entities. Individually identifiable health information (IIHI), including demographics, is protected under HIPAA. This rule covers protected health information (PHI) stored or transmitted in any form or medium - electronic, paper, and oral. It is not limited to documents contained in the official medical record.

Health information covered by the HIPAA Privacy provisions may not be used for purposes not related to health care without explicit authorization from the individual. In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of a medical record for treatment purposes because physicians, specialists, and other providers need access to the full record to provide quality care.

HIPAA increases the patient's control over his/her health information. The patient has a right to:

- A written notice of privacy practices (NOPP) from health plans and providers
- Access, inspect and obtain a copy of PHI
- Request an accounting of disclosures
- Request amendment or correction of their records
- Request restrictions on uses and disclosures of PHI
- Accommodation of reasonable communications requests
- Authorize use or disclosure of PHI for purposes other than Treatment, Payment, and Health Care Operations (TPO)
- Complain to the covered entity and to HHS

All DOD organizations that handle individually identifiable health information are subject to the use and disclosure standards of the Privacy Rule. The Health and Human Services' Office of Civil Rights enforces the Privacy Rule. Penalties for non-compliance with the HIPAA Privacy Rule may apply to the individual violator, head of an organization, or the organization. Civil monetary penalties will be incurred on a per person, per violation basis. Fines and prison terms may result for misuse of patient information with knowledge and intent.

MHS Implementation Plan**TRICARE Management Activity (TMA) Planning Teams**

The TRICARE Management Activity (TMA), Information Management, Technology and Reengineering, electronic Business, Policy and Standards (eBPS) Division is tasked with planning and overseeing DOD's implementation of the HIPAA. To assist in this effort, TMA has chartered a cross-functional HIPAA Overarching Integrated Project Team (OIPT), chaired by the Director eBPS, with members from the Uniformed Services and the Office of General Counsel. The Privacy Working Integrated Project Team (WIPT) is chartered under the OIPT to address standards Privacy Rule.

Army Medical Department (AMEDD) Planning Teams

The AMEDD Chief Information Officer (CIO) is tasked with planning and overseeing the AMEDD's implementation of HIPAA. Similar to TMA, MEDCOM HQ/OTSG has chartered a cross-functional team to assist in this effort. The Deputy CIO chairs the AMEDD Overarching IPT, with members from the functional areas and the MEDCOM Major Subordinate Commands. The AMEDD is coordinating Privacy Rule implementation through the use of its OIPT and separate Privacy WIPT to address compliance requirements. The Deputy Chief, Patient Administration Division (PAD), chairs the AMEDD Privacy WIPT, with members from the MEDCOM Major Subordinate Commands.

Medical Treatment Facility (MTF)/Dental Treatment Facility (DTF) Planning Teams

The MTFs/DTFs will assign a HIPAA Compliance Manager and charter a cross-functional HIPAA Implementation Team to plan and oversee the MTF/DTF's implementation effort. As previously directed, the appointed MTF/DTF Privacy Officer should be a member of the HIPAA Implementation Team.

Compliance Initiatives

There are several initiatives and tools established to assist the military treatment facilities in implementing the Privacy Rule. A summary of these resources follows:

- Draft DOD Health Information Privacy Regulation
 - Prescribes the uses and disclosures of PHI
 - Applies to all organizational entities within the DOD
 - Being revised to include Privacy Rule Amendments
 - Final publication projected 15 November 2002
 - Effective date is 14 April 2003
 - Draft copy provided to RMC and MTF POCs 15 September 2002
- MHS Notice of Privacy Practices (NOPP)
 - Describes beneficiary health information privacy rights and uses/ disclosures of their PHI
 - Will be mailed to TRICARE beneficiaries (head of household) starting on/about 30 November 2002 and ending before 14 April 2003
 - Effective date is 14 April 2003
 - Copy of NOPP provided to RMC and MTF POCs 15 September 2002

- Medical Record Sticker for Patient Acknowledgement
 - MTFs/ DTFs responsible for obtaining acknowledgement of receipt of NOPP
 - Staffed with the Medical Records Consultant to The Surgeon General
 - Serves to permanently record patient (guardian) demographics and signature
 - Interim procedure pending automated (DEERS-CHCS) solution
 - Draft copy will be available to MTFs on or about 30 October 2002
 - Final copies will be available to MTFs on or about 30 November 2002
- Job Description for Privacy Officer
 - Describes roles and responsibilities of Privacy Officer
 - Sent to MEDCOM RMCs/ RDCs with cover memorandum on 20 August 2002
- Web-based HIPAA Awareness Comprehensive e-Learning, testing and tracking tool
 - Purchased by TMA for use throughout DOD
 - Courses organized into 2 levels (Privacy Awareness & Job Specific Training)
 - "Train-the-Trainer" 3 day sessions conducted in September 2002.
 - Limited application available to Privacy Officers in mid- October 2002
 - Fully operational tool will be deployed mid-December 2002
 - Updates on status posted on TMA HIPAA Web Site - www.tricare.osd.mil/hipaa
 - Online demo available at www.quickcompliance.net
- Web-based gap analysis/compliance tool with 230 standards and 3,000 associated tasks (Note: Privacy Rule = 65 standards and 666 associated tasks)
 - Purchased by TMA for use throughout DOD
 - Tool generates a wide array of reports to monitor progress toward compliance
 - Provides continuous upgrades as regulations change
 - "Train-the-Trainer" 3 day sessions conducted in September 2002.
 - Fully operational tool will be deployed mid-December 2002
 - Updates on status posted on TMA HIPAA Web Site - www.tricare.osd.mil/hipaa
 - Online demo available at www.hipaabasics.net
- Business Associate Standard Contract Language
 - Sample contract language binding associates to uphold HIPAA standards on use/ disclosure of PHI
 - MTFs/ DTFs responsible for including this language in applicable affiliations
 - Will be available to MTFs on or about 30 October 2002

Instructions –Timeline Matrix

The AMEDD plan for implementation of the Privacy Rule is structured in accordance with the Department of Defense implementation framework. This will facilitate tracking and reporting of critical compliance objectives as required. The Timeline Matrix on the following page outlines key Privacy milestones and summarizes instructions MTF and DTF commanders may use in developing their implementation plan.

MILESTONES	MHS PLAN /INITIATIVES	TIMELINE	AMEDD PLAN /INITIATIVES	TIMELINE	MSCs/MTFs/DTFs Guide	TIMELINE
HIPAA Work Teams	Establish TMA Privacy WIPT	10-Mar-00	Direct RMC/ MTF to establish HIPAA Planning Implementation team Establish AMEDD Privacy WIPT	8/21/2000 6/15/2002	Establish internal HIPAA Planning /Implementation Team	30-Nov-00
Planning Meetings	Conduct Working Meetings with Service Representatives as required	As Required	Conduct Working Meetings with RMC and MSC Reps as needed	As Required	Conduct Working meetings with subordinate unit HIPAA Reps/ MTF planning team	As Required
Required Reports	Establish reporting requirements	15-Dec-02	Submit required reports to TMA	As Required	Submit required reports to MEDCOM	As Required
Privacy Officer Appointment (Role and Responsibilities)	Direct Service SGs to Appoint Privacy Officer at each MTF/DTFs	18-Jun-02	Direct RMC/ RDCs to Appoint Privacy Officer at each MTF/DTFs	20-Aug-02	Appoint Privacy Officers for each MTF/DTF and integrate in HIPAA Team; reference job description	10-Sep-02
Privacy Officer Training	Conduct HIPAA awareness training to designated MHS HIPAA Planners and Privacy Officers	26-Sep-02	Fund designated AMEDD HIPAA POC to attend HIPAA awareness training	26-Sep-02	Designate staff to attend HIPAA awareness training	26-Sep-02
Privacy Regulation	Develop/staff draft Privacy Regulation prescribing use disclosure of PHI by DOD organization Publish Final version of Regulation	Jan-Jul 02	Staff draft DOD Regulation Develop Army Privacy Regulation prescribing use/disclosure of PHI by AMEDD organization	Jan-Jul 02 15 Nov 02	Reference Draft and Final DOD and Army Privacy Regulations to direct implementation activities	As available
Contract Personnel Support	Provide funding to Services for procurement of contract resources	20-Mar-02	Procure contract personnel to assist AMEDD MSC with HIPAA implementation activities	28-Sep-02	Integrate contract HIPAA consultant into MTF / DTF HIPAA program to accomplish compliance objectives, tasks, other requirements directed by MEDCOM	30-Oct-02
Workforce Education	Purchase Web-based comprehensive e-learning, testing, tracking tool for DOD-wide use Deploy customized tool	20-Aug-02 15-Oct-02 15-Dec-02	Assist in customizing web-based tool for AMEDD organizations, job roles and functional groups	Aug-Oct 02	Develop plan to train workforce using the DOD-purchased web-based tool and other education media as required Complete workforce training	30-Oct-02
Marketing Initiatives	Develop & post HIPAA Privacy marketing materials (posters, tri-folds, flyers) on web-smart site for DOD-wide use	1-Nov-02	Track, notify, assist MSCs to obtain HIPAA Privacy marketing materials for reproduction/ distribution to local community	1-Nov-02	Use DOD web-smart site to order marketing materials to educate the local community & post throughout MTFs as required by Privacy Rule	As available
Notice To Patients	Develop Notice of Privacy Practice (NOPP). Mass mail NOPP to all MHS beneficiaries using address in DEERS database	May-Aug 02 30-Nov-02	Staff Draft NOPP Inform RMCs/MTFs of mailing progress to ensure timely preparation for receipt of patient acknowledgement	15-Aug-02 30-Nov-02	Review and familiarize MTF staff with content of NOPP to ensure appropriate response to patients' concerns	Sep-Nov 02

MILESTONES	MHS PLAN /INITIATIVES	TIMELINE	AMEDD PLAN /INITIATIVES	TIMELINE	MSCs/MTFs/DTFs Guide	TIMELINE
Patient Acknowledgement	Develop medical record stickers to record patient acknowledgement signature Distribute stickers to Services Coordinate DEERS / CHCS SCR to establish automated acknowledgement	May-Oct 02 10-	Collaborate to develop of Medical record stickers and DEERS - CHCS system change coordination Assist MTF/DTFs in obtaining medical record stickers	May-Oct 02 10-Nov-02	Develop plan for receipt of patient acknowledgement signatures using medical records sticker (pending automated solution -DEERS-CHCS)	18-Nov-02
Standard Contract Language for Business Associates	Develop and distribute standard language for Business Associate contracts / MOAs / MOUs	30-Oct-02	Direct (Memo) use of HIPAA standard contract language in applicable Business Association affiliations	30-Oct-02	Include standard HIPAA Privacy contract language in locally established Business Agreements	As available
GAP Analysis-- Policy Revision	Complete GAP analysis of DOD Regulations / policies to HIPAA standards Develop DOD policy where gap exist	10-Jan-03 ASAP	Distribute to MSCs completed GAP analysis of Army Regulations / policies to HIPAA rule Coordinate development of Army policy where gap exists	10-Jan-03 ASAP	Use AMEDD gap analysis to guide compliance assessment Complete GAP analysis of local regulations/policies to HIPAA standards Develop local policies where gap exists.	10-Jan-03 1-Feb-03 ASAP
Monitoring Compliance	Purchase web-based gap analysis tool to monitor DOD-wide progress towards compliance with 65 Privacy standards. Deploy customized web-based tool	20-Aug-02 15-Dec-02	Assist in customizing web-base tool to enable MTF / RMC / MEDCOM to track & report compliance progress with 65 Privacy standards	Aug-Dec 02	Utilize DOD purchased web-base compliance tool to assess, track & report progress towards compliance with 65 Privacy standards	10-Dec-02
Evaluation Metrics			Identify Privacy compliance metrics that support the AMEDD Balanced Score Card (BSC) objectives /targets	15-Jan-03		
Reference Web-Sites	http://www.tricare.osd.mil www.hipaamail@tma.osd.mil Online Demo: www.hipaabasics.net		http://www.us.army.mil > Collaborate >MEDCOM Community >Information Management >HIPAA			

A-6-6

**APPENDIX A-7. Documenting Acknowledgement of
Military Health System (MHS) Notice of Privacy Practice (NOPP).**



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL COMMAND
2050 WORTH ROAD
FORT SAM HOUSTON, TEXAS 78234-6000

MCHO-CL-P

12 Feb 03

MEMORANDUM FOR

COMMANDERS, MEDCOM REGIONAL MEDICAL/DENTAL COMMANDS
COMMANDER, 18th MEDICAL COMMAND, UNIT 15281, APO AP 96205-0054

SUBJECT: Documenting Acknowledgment of Military Health System (MHS) Notice of Privacy Practice (NOPP)

1. The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, requires that every medical and dental treatment facility (MTF/DTF) maintain evidence that beneficiaries received the MHS NOPP. The enclosed NOPP Acknowledgement Label was developed for this purpose. This memorandum provides instructions for the use and disposition of this label.

2. The NOPP explains to beneficiaries how MTFs and DTFs use protected health information and patient rights concerning medical information. In collaboration with the Services, the TRICARE Management Activity (TMA) developed a single NOPP and NOPP Acknowledgement Label for use throughout the MHS. In time to meet the 14 April 2003 compliance deadline, TMA will mail the NOPP to all beneficiaries and provide additional copies to MTFs and DTFs. If the patient requires the MHS NOPP in a different language, the MTF/DTF staff can download the needed version from the TMA website at <http://www.tricare.osd.mil/hipaa>.

3. Sufficient quantities of NOPP Acknowledgement Labels will be mailed by TMA to all MTFs and DTFs no later than 14 February 2003. The MTF/DTF staff may order additional supplies of the label at no cost through the TMA Smart site: <http://www.tricare.osd.mil/smart>.

4. Without exception, the NOPP Acknowledgement Label is the only official document for recording patient signature to verify receipt of the NOPP. The Label must be affixed to the medical record jacket (either DA Form 3444-series or 8005-series), centered on the outside of the back cover, as illustrated at the enclosure. A future update to Army Regulation 40-66, Medical Record Administration and Health Care Documentation, will reflect these changes.

5. I expect every MTF and DTF commander to place the necessary emphasis on this effort to achieve compliance.

A-7-1

DASG-HS

SUBJECT: Documenting Acknowledgment of Military Health System (MHS) Notice of Privacy Practices (NOPP)

6. My project officers are LTC Marta Davidson, AMEDD HIPAA Privacy Project Officer, at DSN 471-6113, COM (210) 221-6113; and Mrs. Teresa Foley, Office of The Surgeon General Medical Record Consultant, DSN 761-3109, COM (703) 681-3109.

FOR THE COMMANDER:



Encl

KENNETH L. FARMER, JR.
Major General
Chief of Staff

Instructions and Sample Plan for Obtaining the Notice of Privacy Practices (NOPP) Acknowledgement Signature

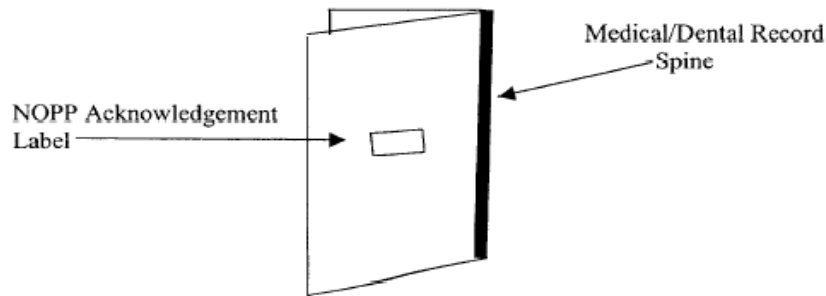
PROCESS: Placement of the NOPP Acknowledgement Label on the outpatient medical/dental Record. The NOPP Acknowledgement Label is not placed on the inpatient medical record.

1. The NOPP Acknowledgement Label shown below was approved by TMA and is the standard form that **MUST** be used within the MHS to verify receipt of the MHS NOPP. An initial supply of labels will be mailed to each MTF/DTF by TMA starting in December 2002. The MTF/DTF is responsible for ordering additional supplies of labels from the TMA SMART site <http://www.tricare.osd.mil/SMART> or they can be locally reproduced from the templates provided by the AMEDD.

Acknowledgement of Military Health System Notice of Privacy Practices	
The signature below only acknowledges receipt of the Military Health System Notice of Privacy Practices, effective date <u>14 April 2003</u> .	
Print Signature of Patient /Patient Representative	date
Name of Patient /Representative	relationship to patient (if applicable)
FMP/SSN: / - -	
<input type="checkbox"/> Patient/Representative declined to sign MTF staff initials	

Note: The label is sized to scale and can be reproduced locally on Avery Label #5263, size: 2 inches x 4 inches. TMA has provided a template for local reproduction of the label, if the MTF/DTF desires to use this approach.

2. The MHS NOPP Acknowledgement Label **MUST** be placed on the **BACK OUTSIDE COVER** of the outpatient medical/dental record, **CENTERED IN THE MIDDLE** of the records jacket.

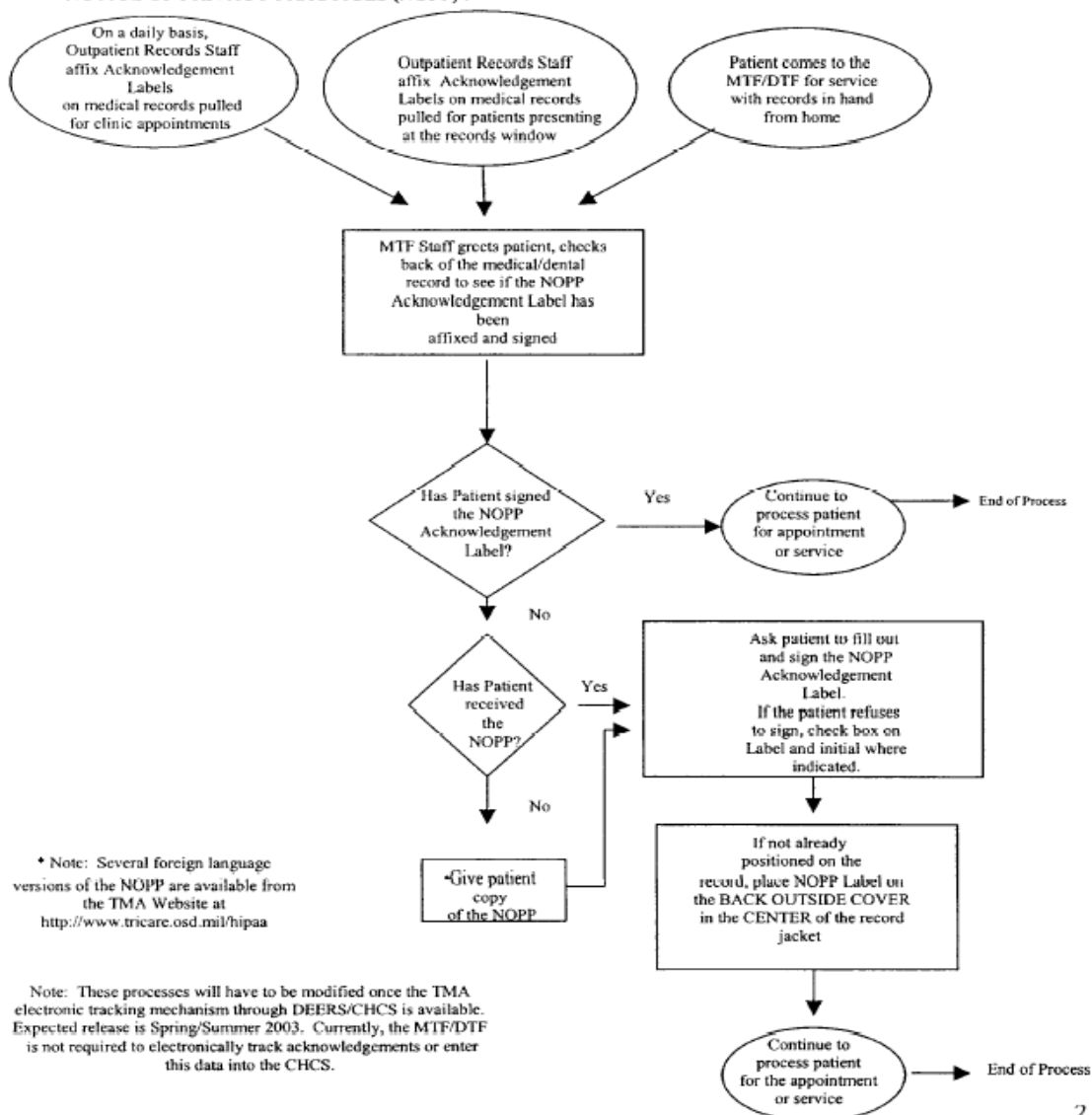


3. Wherever possible, the staff of the MTF/DTF Medical Records Department should affix the label on the medical/dental record **PRIOR TO THE PATIENT'S APPOINTMENT**. This approach reduces the administrative burden in the clinical and patient care areas.

4. Suggested locations within the MTF/DTF where patients may be requested to sign the label include, but are not limited to: outpatient records window, clinic reception areas, Patient Representative's Office, admissions and disposition waiting area, pharmacy reception areas (pharmacy window not recommended), or other appropriate areas within the MTF/DTF where patients present for treatment or service.

5. Patients who maintain their medical/dental records at home and come to the MTF/DTF for care/service without their outpatient medical/dental record must be reminded that the medical/dental record is government property and asked to return the record to the facility.

SUGGESTED PROCESS FOR OBTAINING PATIENT SIGNATURE TO ACKNOWLEDGE RECEIPT OF THE MHS NOTICE OF PRIVACY PRACTICES (NOPP) :



APPENDIX A-8. Data Call for Systems Transmitting HIPAA Electronic Transactions.REPLY TO
ATTENTION OF**DEPARTMENT OF THE ARMY**
OFFICE OF THE SURGEON GENERAL
5109 LEESBURG PIKE
FALLS CHURCH VA 22041-3258

S: 21 April 2003

DASG-IMD

24 March 2003

MEMORANDUM FOR SEE DISTRIBUTION**SUBJECT:** Data Call for Systems Transmitting Health Insurance Portability and Accountability Act (HIPAA) Electronic Transactions

1. The Health Insurance Portability and Accountability Act, Standards for Electronic Transactions Regulation, requires the use of standard formats for select health care administrative and financial transactions. The types of transactions impacted by this HIPAA rule include health care claims, payment for care, coordination of benefits, claim status, enrollment, health plan eligibility, health plan premiums, referral certification and authorization, first injury reports, and health claim attachments.
2. This data call is to identify the systems that are currently sending or receiving the transactions identified in paragraph 1. Once the systems are identified, we will work with the program managers to make these systems HIPAA compliant. The instructions and format for this data call are at Enclosure 1 and 2, respectively. Please provide your submissions electronically to our point of contact (POC) not later than 21 April 2003.
3. Our POC is Ms. Theora L. Mitchell, Contractor, Office of the Assistant Chief of Staff for Information Management, DSN 471-8347, Commercial (210) 221-8347, or electronic mail theora.mitchell@amedd.army.mil.

FOR THE SURGEON GENERAL:

- 2 Encls
1. Data Call Instructions
 2. Data Call Format

KENNETH L. FARMER, JR., M.D.
Major General
Deputy Surgeon General

[illegible]

APPENDIX A-9. HIPAA Training Requirements.REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, U. S. ARMY MEDICAL COMMAND
2050 WORTH ROAD, SUITE 10
FORT SAM HOUSTON, TEXAS 78234-6010

S: 14 May 03

MCHO-CL-P

28 April 2003

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Health Insurance Portability and Accountability Act (HIPAA) Training Requirements

1. One of the obligations facing AMEDD organizations under the HIPAA Privacy Rule is providing an on-going and effective training program to members of the workforce. Despite a good effort, the AMEDD did not meet full compliance with this requirement by the 14 April 2003 deadline (enclosure 1). This memorandum clarifies the training requirement and establishes a new compliance deadline for AMEDD organizations.
2. I ask each organization affected by HIPAA requirements to redouble their efforts ensuring individuals such as employees, contractors, volunteers, and business associates understand what they can and cannot do under the HIPAA law and why. Medical and dental treatment facilities are required to train all of their workforce. Other major subordinate commands are required to train members who have direct or indirect contact with protected health care information in the course of their duties and responsibilities.
3. In response to your frustrations with the dedicated web-based training tool problems, I wrote TMA and laid out the MEDCOM's concerns. TMA acknowledged the problems and has been systematically correcting them; improvement will be ongoing and continuous. Commanders are responsible for ensuring that personnel operating the web-base program adhere to the established business rules. The business rules and instructions for completing the web base training are outlined in enclosure 2.
4. I expect all commanders to reach compliance with all HIPAA requirements no later than 14 May 2003. Our success and the key to achieving and maintaining compliance with the HIPAA law will ultimately depend on how well we prepare our personnel.

FOR THE COMMANDER:

2 Encls (removed)

KENNETH L. FARMER, JR.
Major General
Chief of Staff

DISTRIBUTION:
COMMANDERS, MAJOR MEDICAL REGIONAL COMMANDS/ACTIVITIES/INSTALLATIONS
DIRECTORS, OTSG/MEDCOM

BUSINESS RULES FOR THE WEB BASE HIPAA TRAINING TOOL

The following are instructions, keys to success, for MTF Privacy Officers and HIPAA training tool system administrators.

- The training tool requires the use of Internet Explorer 5.5 or higher (do not use Netscape)
- Users must register using their .mil email address, even if accessing the tool from their private (home) internet account.
- A Quick Start Guide has been provided to all Privacy Officers (copy Attached). Privacy Officers must provide a copy of this guide to all users to assist them in the registration process. *(Note: Quick Start Guide removed from this AMEDD Implementation Guide; updated copy available at <http://tricare.osd.mil/hipaa/Training-and-Compliance.htm>)*
- Prior to registration it is especially important for Privacy Officers to provide the "domain" name for their unit, and remind all users to remember their system-generated student identification number and their self-designed password. Without these two items users will not be able to re-enter the tool to complete any training modules not finished in earlier sessions.
- Once in the training tool, students must use the "Exit" button in the Course content (Not the web browser's Exit button) to receive full credit for completion of online courses. The "Exit" button is located on the main menu page at the bottom right corner, and the training application itself provides detailed instructions on the screen.
- In some cases the settings on a particular computer may not open the training application screen to the full size and thereby not make this Exit button visible. If this is the case, remind users to simply hit the "F11" key to open the screen to full size.
- If student identification numbers or passwords are forgotten, please remind users that their local HIPAA training tool system administrator can reset passwords, unlock accounts and retrieve student IDs. To facilitate the fastest resolution, the local MTF HIPAA training tool system administrator should be the first point of contact for these sorts of problems, not the HIPAA Help Desk.
- The Privacy Officer must identify the local system administrator for users.
- When local system administrators access the training application however, it is absolutely critical that they do not delete or modify in any way the student record titled "SHUTS DOWN ENTIRE MHS!, DO NOT MODIFY OR DELETE THIS RECORD!!! DO NOT MODIFY". Any changes to this record will shut down new user registration for the entire MHS.

- Remind users that this is a web-based system that can be accessed from any computer (using Internet Explorer 5.5 or higher) on a 24/7 basis. If during log-in or registration a user receives a "404" error, it is because the tool is waiting for an opportunity to add an additional participant. Using the 'Refresh' button on the web browser or hitting the F5 key will reload the registration screen and/or log-in page.

APPENDIX A-10. Data Call to Assess HIPAA Privacy Rule Compliance.

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MEDICAL COMMAND
2050 WORTH ROAD
FORT SAM HOUSTON, TEXAS 78234-6013

REPLY TO
ATTENTION OF

S: 05 May 2003

MCIM

21 APR 2003

MEMORANDUM FOR Commanders, U.S. Army Medical Command Regional Medical Commands

SUBJECT: Data Call to Assess Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance

1. References:

a. DoD Regulation 6025.18-R, DoD Health Information Privacy Regulation, 24 January 2003.

b. Headquarters, U.S. Army Medical Department (AMEDD) Health Insurance Portability and Accountability Act (HIPAA) Implementation Guide, Version 1.0, 6 January 2003.

2. The 14 April 2003 deadline for compliance with the HIPAA Privacy Rule has occurred and we are conducting a data call to assess the level of compliance in Army medical and dental treatment facilities. This data call will focus on the major administrative requirements addressed in reference 1a. These requirements are as follows:

- a. Appoint a privacy official.
- b. Train the workforce.
- c. Establish policy regarding special rules and requirements for the use and disclosure of Protected Health Information (PHI). Includes de-identification of PHI, minimum necessary rule, limited data sets, etc.
- d. Establish policy regarding an individual's rights to request privacy protection for PHI, to include requests for restrictions and communications by alternative means and at alternative locations.
- e. Establish a system for the accounting of disclosures of PHI.
- f. Establish policy regarding access to and amendment of PHI.

MCIM

SUBJECT: Data Call to Assess Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance

g. Insert standard HIPAA Privacy Rule contract language in new business associate (BA) agreements and the existing BA agreements that were renewed or modified between 15 October 2002 and 14 April 2003.

h. Establish a complaint and inquiry system.

i. Establish a system of sanctions against members of the workforce who fail to comply with HIPAA privacy policies and procedures.

j. Establish policy to implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

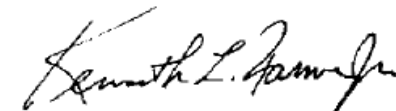
3. The data call instructions and worksheets are at Enclosures 1 and 2, respectively. Please complete the data call worksheet and validate the accuracy of this report by signing the certificate of compliance at Enclosure 3. Submit the data call worksheet and the certificate of compliance not later than 05 May 2003 to Ms. Theora L. Mitchell, Contractor, Office of the Assistant Chief of Staff for Information Management, DSN 471-8347, facsimile (FAX): DSN 471-8518, or electronic mail (e-mail): Theora.Mitchell@amedd.army.mil. The data call worksheet should be sent electronically. The certificate of compliance may be sent electronically or by FAX.

4. Our point of contact is LTC Marta Davidson, AMEDD HIPAA Privacy Project Officer, DSN 471-6113 or e-mail: Marta.Davidson@amedd.army.mil.

FOR THE COMMANDER:

3 Encls

1. Data Call Instructions
2. Data Call Worksheets
3. Certificate of Compliance



KENNETH L. FARMER, JR.
Major General
Chief of Staff

CF: Commander, 18th Medical Command, Unit 15281, APO AP 96205-0054

APPENDIX A-11. Compliance of MEDCOM Agreements with the HIPAA.

REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL COMMAND
2050 WORTH ROAD
FORT SAM HOUSTON, TEXAS 78234-6000

MCRM-M

04 JUL 2003

MEMORANDUM FOR

Commanders, MEDCOM Major Subordinate Commands
Chiefs, Staff Offices

SUBJECT: Compliance of U.S. Army Medical Command (MEDCOM) Agreements with the Health Insurance Portability and Accountability Act (HIPAA)

1. References.

- a. DOD Regulation 6025-18, DOD Health Information Privacy Regulation, 24 January 2003.
- b. U.S. Army Medical Department (AMEDD) HIPAA Implementation Guide (Version 1), 6 January 2003.

2. The HIPAA Privacy Rule requires AMEDD organizations that generate or maintain protected patient information to establish written privacy assurances with Business Associates who may be exposed to this information. The requirement for privacy assurances extends to arrangements between the MTF and other parties that are formalized as Affiliation Agreements, Gratuitous Agreements, support agreements, and memoranda of agreement or understanding (MOAs or MOUs). This memorandum clarifies compliance requirements of the law as related to MEDCOM agreements entailing use of protected health information.

3. Reference 1a., above, establishes the privacy standards applicable to all Department of Defense (DOD) organizations that handle protected patient information.

- a. If all parties in the agreement are components of DOD, the agreement must annotate Reference 1a., above, as the regulatory guide for privacy standards.

- b. If any party in the agreement is non-DOD (either intra-governmental or nongovernmental), the written agreement must include explicit language assuring protection of patient information in accordance with the HIPAA Privacy Rule.

4. Implementation instructions and a privacy clause template are enclosed. All agreements that require privacy assurance must be compliant no later than 14 April 2004; however, any agreement in place before 15 October 2002, but renewed or modified between 15 October 2002 and 14 April 2003, must be made compliant immediately.

MCRM-M

SUBJECT: Compliance of U.S. Army Medical Command (MEDCOM) Agreements with the Health Insurance Portability and Accountability Act (HIPAA)

5. Our points of contact are Mr. Brian Clearman, Office of the Assistant Chief of Staff for Resource Management, DSN 471-7036 or Commercial (210) 221-7036; LTC Marta Davidson, MEDCOM HIPAA Privacy Program Manager, DSN 471-6113 or Commercial (210) 221-6113; and Mr. Charles Orck, Office of the Staff Judge Advocate, DSN 471-8400 or Commercial (210) 221-8400.

FOR THE COMMANDER:

Encl


KENNETH L. FARMER, JR.
Major General
Chief of Staff

INSTRUCTIONS FOR ESTABLISHING AGREEMENTS IN COMPLIANCE WITH THE HIPAA PRIVACY RULE

1. The following guidelines apply only to agreements involving the use or disclosure of protected health information (PHI).
2. There are two essential elements of compliance for this requirement. First, all agreements that entail the use or disclosure of PHI must be in writing. Second, the agreement must incorporate language that describes the responsibility of each partner to safeguard the medical information as related to the business endeavor. That language must be provided by the party maintaining the PHI.
3. The following are examples of agreements that require a privacy clause in accordance with the HIPAA Privacy Rule:

a. TRAINING AGREEMENTS.

(1) Gratuitous Agreements, Medical Training Agreements, and Educational Service Agreements (i.e., AMEDD personnel who train at civilian institutions): In these types of agreements, the AMEDD organization is the Business Associate who must provide assurance, as directed by the civilian institution, to protect patient information generated or maintained at the civilian institution. It is therefore incumbent upon the civilian institution to provide its own approved privacy clause for incorporation to the agreement.

(2) Affiliation Agreements (i.e., non-DOD personnel from civilian institutions who train at AMEDD organizations): All Affiliation Agreements are developed by the sponsoring AMEDD organization and must include a Privacy Clause assuring that trainees from affiliated civilian institutions who train in AMEDD facilities will comply with privacy standards.

b. MEMORANDA OF UNDERSTANDING/AGREEMENT (MOUs/MOAs), INTERSERVICE SUPPORT AGREEMENTS (ISSA), INTERAGENCY AGREEMENTS (IA), and SUPPORT AGREEMENTS (DD Form 1144): Specifically when these agreements include a non-DOD party, the party that maintains the PHI is responsible for incorporating language in the agreement assuring that all parties will comply with privacy standards as required by law.

4. The following privacy template language may be used in the agreements listed above.* All agreements that require privacy assurance must be compliant NLT 14 April 2004; however, any agreement in place before 15 October 2002, but renewed or modified between 15 October 2002 and 14 April 2003, must be made compliant immediately.

* NOTE: The recommended and preferred way to meet the requirement is by inserting the specified privacy clause in any new or revised agreements. An alternate, but less preferred, method is to add the privacy clause in a separate addendum to the agreement, should amending an existing agreement not be deemed in the best interest of the Army. If an addendum is added, annotate the original agreement to reflect establishment of the addendum.

ENC1

BUSINESS ASSOCIATE PRIVACY CLAUSE***Privacy of Protected Health Information (PHI)**

1. Terms used in this section shall have the same meaning as those terms in 45 CFR 160 and/or DOD Regulation 6025-18, DOD Health Information Privacy Regulation.
2. Obligations and Activities of Business Associate. The Business Associate:
 - a. Will not use or disclose PHI other than as permitted or required by agreement or Law.
 - b. Will use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this agreement (specify type of agreement such as MOA, Affiliation Agreement, etc.).
 - c. Will report to the sponsoring AMEDD organization (Covered Entity) any use or disclosure of the PHI not provided for by this agreement.
 - d. Will mitigate, as practicable, any harmful effect known to the Business Associate of use or disclosure of PHI by the Business Associate in violation of the requirements of this agreement.
3. Except as otherwise limited in this agreement, the Business Associate:
 - a. May use or disclose Protected Health Information to perform functions or services for, or on behalf of, Covered Entity as specified in this agreement, provided that such use or disclosure would not violate the Privacy Rule if done by the Covered Entity.
 - b. May use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
 - c. May disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
4. Obligations of Covered Entity. The Covered Entity:
 - a. Upon request shall provide the Business Associate with the notice of privacy practices that the Covered Entity produces, as well as any changes to such notice.
 - b. Shall provide the Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.
 - c. Shall notify the Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to IAW 45 CFR 164.522.

*Incorporate above clause in agreement and format as appropriate by compliance deadline.

APPENDIX A-12. Interim Forms for Authorization and Restriction of PHI.REPLY TO
ATTENTION OF**DEPARTMENT OF THE ARMY**
OFFICE OF THE SURGEON GENERAL
5109 LEESBURG PIKE
FALLS CHURCH, VA 22041-3258

DASG-HS

03 JUL 2003**MEMORANDUM FOR****COMMANDERS, MEDCOM REGIONAL MEDICAL/DENTAL COMMANDS;
COMMANDER, 18TH MEDICAL COMMAND, UNIT 15281, APO AP 96205****SUBJECT: Interim Forms for Authorization and Restriction of Protected Health Information**

1. This memorandum provides instructions for the interim use of two template forms to meet Health Insurance Portability and Accountability Act (HIPAA) requirements: Authorization For the Use and Disclosure of Medical and Dental Information and Request To Restrict Medical or Dental Information.
2. Pending publication as Department of Defense (DD) Forms, medical and dental treatment facilities (MTF and DTF) commanders must use the two templates at the Enclosure in place of DA Form 5006 (Medical Record–Authorization for Disclosure of Information).
3. When published, the DD Forms will replace the templates and the DA Form 5006. In the interim, MTF and DTF Commanders should assign a local form number to both templates for accountability. Both forms should be filed in the same location as indicated for DA Form 5006 in AR 40-66 dated 28 March 2003.
4. My project officers are LTC Marta Davidson, HIPAA Privacy Project Manager, DSN 471-6113, and Ms. Teresa Foley, Medical Records Consultant, DSN 761-3109.

FOR THE SURGEON GENERAL:2 Encls
as

A handwritten signature in black ink, reading "Kenneth L. Farmer, Jr.", is positioned above the printed name.

KENNETH L. FARMER, JR.
Major General
Deputy Surgeon General

AUTHORIZATION FOR DISCLOSURE OF MEDICAL OR DENTAL INFORMATION		
<p>The purpose of this form is to provide the MTF/DTF/TRICARE Health Plan with a means to request the use and/or disclosure of an individual's protected health information. Guidelines regarding use of this form are contained in DOD Regulation 6025.18-R.</p> <p>This form will not be used for authorization to disclose alcohol or drug abuse patient information from medical records or for authorization to disclose information from records of an alcohol or drug abuse treatment program. In addition, any use as an authorization to use or disclose psychotherapy notes may not be combined with another authorization except one to use or disclose psychotherapy notes.</p> <p>Privacy Act of 1974 applies.</p>		
PATIENT DATA		
Name (Last, First, MI)	Date of Birth (YYYYMMDD)	Patient SSN
Period of treatment (YYYYMMDD - YYYYMMDD)	Type of Treatment: <input type="checkbox"/> Outpatient <input type="checkbox"/> Inpatient <input type="checkbox"/> Both	
DISCLOSURE		
<p>I authorize _____ (Name of MTF/DTF/TRICARE Health Plan) to release my patient information to:</p> <p>Name _____</p> <p>Address _____ City _____ State _____ Zip _____</p> <p>Phone _____ Fax _____</p>		<p>Reason for Request/Use of Medical Information:</p> <p><input type="checkbox"/> Personal Use</p> <p><input type="checkbox"/> Insurance</p> <p><input type="checkbox"/> Continued Medical Care</p> <p><input type="checkbox"/> School</p> <p><input type="checkbox"/> Legal</p> <p><input type="checkbox"/> Retirement/Separation</p> <p><input type="checkbox"/> Other (please specify) _____</p>
Information to be Released:		
Authorization Start Date (YYYYMMDD):		<p>Authorization Expiration:</p> <p><input type="checkbox"/> Date (YYYYMMDD) _____</p> <p><input type="checkbox"/> Action Completed</p>
RELEASE AUTHORIZATION		
<p>I understand that:</p> <p>a. I have the right to revoke this authorization at any time. My revocation must be in writing and provided to the facility where my medical records are kept or to the TMA Privacy Officer if this is an authorization for information possessed by the TRICARE Health Plan rather than an MTF or DTF. I am aware that if I later revoke this authorization, the person(s) I herein name will have used and/or disclosed my protected information on the basis of this authorization.</p> <p>b. If I authorize my protected health information to be disclosed to someone who is not required to comply with federal privacy protection regulations, then such information may be re-disclosed and would no longer be protected.</p> <p>c. I have a right to inspect and receive a copy of my own protected health information to be used or disclosed, in accordance with the requirements of the federal privacy protection regulations found in the Privacy Act and 45 CFR §164.524.</p> <p>d. The Military Health System (which includes the TRICARE Health Plan) may not condition treatment in MTFs/DTFs, payment by the TRICARE Health Plan, enrollment in the TRICARE Health Plan or eligibility for TRICARE Health Plan benefits on failure to obtain this authorization.</p> <p>I request and authorize the named provider/treatment facility/TRICARE Health Plan to release the information described above to the named individual/organization indicated.</p>		
Signature of Patient/Parent/Legal Patient Representative	Relationship to Patient (if applicable)	Date (YYYYMMDD)
<p>For Staff Use Only-(To Be Completed only Upon Receipt of Written Revocation)</p> <p><input type="checkbox"/> AUTHORIZATION REVOKED</p> <p>Revocation completed by _____ Date ____/____/____</p>		
Imprint of Patient Identification Plate When Available	<p>Sponsor Name:</p> <p>Sponsor Rank:</p> <p>FMP/Sponsor SSN:</p> <p>Branch of Service:</p> <p>Phone Number:</p>	

DD FORM XXXX, XXX 2003

DD FORM XXXX, XXX 2003

APPENDIX B. AMEDD HIPAA Overarching Integrated Project Team Charter and Member Information.

CHARTER

U.S. ARMY MEDICAL DEPARTMENT Health Insurance Portability and Accountability Act Overarching Integrated Project Team

Purpose

The Health Insurance Portability and Accountability Act (HIPAA) Overarching Integrated Project Team (OIPT) will develop a compliance strategy and provide oversight of the execution process to ensure that all HIPAA requirements are implemented accurately and in a timely manner. This document replaces the MEDCOM HIPAA IPT Revised Charter signed on 2 May 2002.

Individual Working Integrated Project Teams (WIPTs) and/or sub-work groups will support the HIPAA OIPT as required and report to the HIPAA OIPT on a periodic basis. Initially, a Privacy WIPT will be chartered.

The OIPT Project Manager may task appropriate offices within the U. S. Army Medical Command and Office of the Surgeon General to take the functional lead for various HIPAA requirements.

Membership

Deputy Chief Information Officer (Project Manager for HIPAA)
ACSIM, Security Division Representative
ACSH&S, Patient Administration Division Representative
Medical Records Consultant
ACSH&S, Clinical Services Representative
ACSH&S, TRICARE Division Representative
PASBA Representative
Staff Judge Advocate Representative
ACSPER Representative
ACSRM Representative
FOIA/Privacy Act Representative
MEDCOM Major Subordinate Command Representatives
- Dental Command
- Center for Health Promotion and Preventive Medicine
- AMEDD Center and School
- Medical Research and Materiel Command
- Regional Medical Commands
Reserve Affairs Representative
Army Guard Representative
Additional participants may be added as needed, at the discretion of the Project Manager.

11/13/2002

Meetings

Meetings will be held monthly during the life cycle of the program. The Project manager may adjust this schedule as required. Individual WIPTs and other sub-groups will meet as necessary.

Deliverables

Deliverables will include the following documents:

- Project Management Plan
- Implementation Plan
- Compliance Strategy Plans
- Position or Issue Papers
- Tasking Documents
- Progress Reports

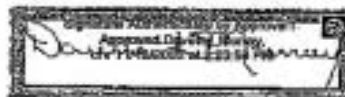
The HIPAA IPT and the WIPT Project Managers will publish approved minutes.

Duration

This charter will be reviewed for resubmission in one year.

Effective Date

This charter becomes effective on the date it is signed by the Deputy Surgeon General.



DAVETTE L. MURRAY
Lieutenant Colonel
Deputy Chief Information Officer/HIPAA Project Manager

Date

Kenneth L. Farmer, Jr. 17 Nov 02
KENNETH L. FARMER, JR., M.D.
Major General
Deputy Surgeon General

Date

AMEDD HIPAA Overarching Integrated Project Team Participants				
Position	Name	Phone	DSN	E-Mail Address
HIPAA Project Manager Deputy CIO	LTC Davette Murray	210-221-8169	471	Davette.Murray@amedd.army.mil
Security WIPT Chairman ACSIM - Chief, Plans and Policies	Mr. Barzie Drewry	210-221-6836	471	Barzie.Drewry@amedd.army.mil
Security Project Manager ACSIM - Alternate IAPM	Mr. Ross Roberts	210-221-7869	471	Ross.Roberts@amedd.army.mil
Privacy WIPT Project Manager Deputy Chief, Patient Administration Div	LTC Marta Davidson	210-221-6113	471	Marta.Davidson@amedd.army.mil
Transactions and Code Sets Project Manager Tertiary Care Staff Officer, Clinical Services Div	LTC Norvell Coots	703-681-0102	761	Norvell.Coots@amedd.army.mil
Medical Records Consultant	Ms. Terry Foley	703-681-3109	761	Teresa.Foley@amedd.army.mil
Clinical Services Division Representative	COL Monica Secula	210-221-7885	471	Monica.Secula@amedd.army.mil
TRICARE Operations Division Representative	Ms. Tama Oringderff	210-221-7217	471	Tama.Oringderff@amedd.army.mil
PASBA Representative	MAJ Deborah Wesloh	210-295-8936	471	Deborah.Wesloh@amedd.army.mil
Staff Judge Advocate Office	Mr. Charles Orck	210-221-8400	471	Charles.Orck@amedd.army.mil
ACSPER Representative	TBD			
ACSRM Representative	LTC Marcus Cronk	210-221-7844	471	Marcus.Cronk2@amedd.army.mil
FOIA/Privacy Act Representative	Mr. John Peterson	210-221-7826	471	John.Peterson1@amedd.army.mil
DENCOM Representative	COL John Storz	210-221-8241	471	John.Storz@amedd.army.mil
CHPPM Representative	Ms. Janet Blackburn	410-436-7222	584	Janet.Blackburn@amedd.army.mil
AMEDDC&S Representative	MAJ Wanda Wade	210-221-8675	471	Wanda.Wade@amedd.army.mil

AMEDD HIPAA Overarching Integrated Project Team Participants				
Position	Name	Phone	DSN	E-Mail Address
MRMC Representatives	Mr. Thomas Lang	301-619-2984	343	Tom.Lang@amedd.army.mil
	Ms. Phylis Rinehart	301-6197547	343	Phylis.Rinehart@amedd.army.mil
ERMC Representatives	LTC Mark Glad	DSN 314-371-2111		Mark.Glad@amedd.army.mil
	Ms. Rebecca Bridges	DSN 314-37131888		Rebecca.Bridges@amedd.army.mil
GPRMC Representative	Mr. Michael Flahie	210-295-2342	421	Michael.Flahie@amedd.army.mil
NARMC Representative	LTC Mary Bedell	202-782-9094	882	Mary.Bedell@amedd.army.mil
PRMC Representatives	CPT Jennifer Gerald	808-433-2327	--	Jennifer.Gerald@amedd.army.mil
	LTC David Gilbertson	808433-5230	--	David.Gilbertson@amedd.army.mil
SERMC Representative	Ms. Rose Reedy	706-787-3568	780	Rose.Reedy@amedd.army.mil
WRMC Representatives	LTC Michael Griffin	253-968-1795	782	Michael.Griffin2@amedd.army.mil
	Mr. John Mares	253-968-1642	782	John.Mares@amedd.army.mil
Reserve Affairs Representative	COL Jane McCullough	210-221-6502	471	Jane.McCullough@amedd.army.mil
Army National Guard Representative	COL Todd Furse	210-221-7905	471	Todd.Furse@amedd.army.mil
ACSIM - Security Branch	Mr. W. Chris Hastedt	210-221-8593	471	William.Hastedt@amedd.army.mil
OIPT Recorder, HIPAA Contract Support	Ms. Theora Mitchell	210-221-8347	471	Theora.Mitchell@amedd.army.mil
OIPT Admin HIPAA Contract Support	Mr. Troy Elms	210-221-8814	471	Troy.Elms@amedd.army.mil
HIPAA Security Contract Support	Ms. Jan Eagan	210-221-8989	471	Janet.Eagan@amedd.army.mil
HIPAA Privacy Contract Support	Mr. Tom Leonard	210-221-7841	471	Tom.Leonard@amedd.army.mil

**APPENDIX C-1. AMEDD HIPAA Transactions and
Code Sets WIPT Team Charter and Member Information.**

CHARTER

**U.S. ARMY MEDICAL DEPARTMENT
Health Insurance Portability and Accountability Act (HIPAA)
Transactions and Codes Sets Working Integrated Project Team**

Purpose

The AMEDD Transactions and Codes Sets (T&CS) Working Integrated Project Team (WIPT) will, working in concert with the Department of Defense T&C Working Integrated Project team (WIPT), develop requirements and an implementation plan for compliance with the T&CS rules of the HIPAA. The WIPT will also provide oversight of the execution process across the AMEDD, to ensure that all requirements are implemented accurately and within the Federally mandated time frame. The AMEDD T&CS WIPT Project Officer will represent the AMEDD during the DoD/Health Affairs/TRICARE Management Agency (DoD/HA/TMA) T&CS WIPT planning meetings, and will ensure that all implementation initiatives include AMEDD requirements.

Core Membership

AMEDD T&CS WIPT Project Officer.....LTC Norvell V. Coots, M.D.

MEDCOM PAD Representative
MEDCOM TRICARE Representative
MEDCOM CSD Representative
MEDCOM IMD Representative
GPRMC Representative
PRMC Representative
ERMC Representative
SERMC Representative
NARMC Representative
WRMC Representative
18th MEDCOM Representative (by invitation)
DENCOM Representative
PASBA Representative

AD HOC Membership

OCAR Representative
NGB Representative
MRMC Representative
AC&S Representative
CHPPM Representative
Additional members may be added at the discretion of the Project Officer.

Meetings

Meetings will be held monthly during the life cycle of the project. The WIPT Project Officer may adjust the schedule as necessary.

Approved minutes will be published and submitted to the AMEDD HIPAA OIPT.

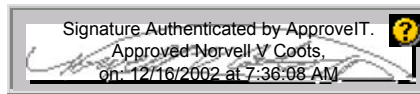
Products

Products generated by this WIPT will include the following:

Implementation Plan
Implementation Timelines
Policy recommendations and guidelines
System Changes and Technical specifications
Acquisition and Budget requirements
Other products as needed.

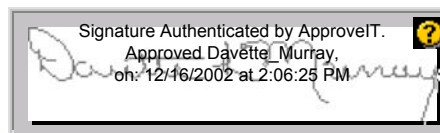
Duration

This charter will be reviewed for resubmission in one year.



Signature Authenticated by ApproveIT.
Approved Norvell V Coots,
on: 12/16/2002 at 7:36:08 AM

NORVELL V. COOTS, M.D. 16 DEC 02
Lieutenant Colonel, Medical Corps
Medical Staff Officer/ HIPAA T&CS WIPT Project Officer



Signature Authenticated by ApproveIT.
Approved Davette Murray,
on: 12/16/2002 at 2:06:25 PM

DAVETTE L. MURRAY 16 DEC 02
Lieutenant Colonel, Medical Service Corps
Deputy CIO/ HIPAA Project Manager

AMEDD HIPAA Transactions and Code Sets Working Integrated Project Team Participants				
Position	Name	Phone	DSN	E-Mail Address
AMEDD HIPAA Transactions and Code Sets Project Manager Tertiary Care Staff Officer, Health Services Division, 0ACSHPS	LTC Norvell Coots	703-681-0102	761	Norvell.Coots@amedd.army.mil
MEDCOM PAD Representative	Mr. Doug Ashby	210-2216113	471	Doug.Ashby@amedd.army.mil
MEDCOM TRICARE Representative	Ms. Tama Oringderff	210-221-7217	471	Tama.Oringderff@amedd.army.mil
MEDCOM IMD Representative	Mr. Robert Collier, Contractor	210-221-7955	471	Robert.Collier@amedd.army.mil
GPRMC Representative	Mr. Michael Flahie	210-221-2342	471	Michael.Flahie@amedd.army.mil
PRMC Representative	Mr. Nash Keel	808-433-1016		hugh.keel@amedd.army.mil
ERMC Representative	Ms. Rebecca Bridges	DSN 96221-17-3166	---	Rebecca.Bridges@amedd.army.mil
SERMC Representative	Ms. Cami Miranda	706-787-0108	780	Camilla.Miranda@amedd.army.mil
NARMC Representative	COL Mary Bedell	202-782-9094	882	Mary.Bedell@amedd.army.mil
WRMC Representative	Ms. Kathy Pegum	253-968-1815	782	Kathy.Pegum@amedd.army.mil
18th MEDCOM Representative	TBD			
DENCOM	MAJ Kyle Campbell	210-829-2904	471	Kyle.Campbell@amedd.army.mil
PASBA Representative	TBD			
USARC Representative	Mr. Bob Rowe	404-464-8040		robert.d.rowe@us.army.mil
NGB Representative	TBD			
MRMC	Mr. Thomas D. Lang	301-619-2984	343	Tom.Lang@us.army.mil
AC&S Representative	TBD			
CHPPM Representative	TBD			
WIPT Recorder	Mr. Stanley Crocker	703-681-1876	761	Stanley.Crocker@amedd.army.mil

C-1-3

APPENDIX C-2. AMEDD HIPAA Privacy WIPT Charter and Member Information.

**CHARTER
U.S. ARMY MEDICAL COMMAND
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
PRIVACY WORKING INTEGRATED PROJECT TEAM (WIPT)**

Purpose:

The Army Medical Department (AMEDD) Privacy Working Integrated Project Team (WIPT) will develop requirements and an implementation plan for compliance with the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) and the Privacy Act of 1974. The Privacy WIPT will examine current AMEDD business processes and recommend a strategy for addressing and integrating requirements for the protection of individually identifiable health information as mandated by HIPAA and the Privacy Act. The AMEDD Privacy WIPT Project Officer will represent the AMEDD during the Health Affairs / TRICARE Management Activity (HA/ TMA) Privacy WIPT planning meetings and will ensure all implementation initiatives sponsored by HA/TMA incorporate AMEDD requirements. The WIPT will monitor implementation activities and report to the AMEDD HIPAA Overarching Integrated Project Team (OIPT) as required.

Core Membership:

AMEDD Privacy WIPT Project Officer-----LTC Marta S. Q. Davidson

MEDCOM /PAD Representative
GPRMC HIPAA Representative
PRMC HIPAA Representative
ERMC HIPAA Representative
SERMC HIPAA Representative
NARMC HIPAA Representative
WRMC HIPAA Representative
18TH MEDCOM Representative
DENCOM Representative
AC&S Representative
MRMC Representative
CHPMM Representative
PASBA Representative
OCAR Representative
NGB Representative
OTSG Representative
AFIP Representative
Freedom of Information Act Representative

Ad Hoc Membership:

Office of General Counsel Representative
MEDCOM UBO Representative

Additional participants may be added as needed, at the discretion of the Privacy WIPT Project Officer.

Meetings:

Meetings will be held monthly during the life cycle of the project. The WIPT Project Officer may adjust this schedule as necessary.

Deliverables:

Deliverables will include the following:

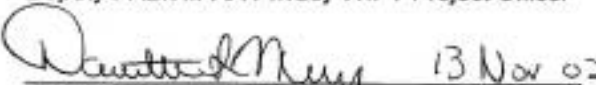
Privacy Regulation Gap Analysis
Functional Requirements Documents
Contract for On-site MTF HIPAA Support
Implementation Plans and Timelines
Acquisition and Budget Requirements
Policy Recommendations and Guidelines
System Changes with Technical Specifications
Other HIPAA Privacy compliance deliverables, as necessary

The Privacy WIPT Project Officer shall publish approved minutes and submit to the AMEDD HIPAA OIPT.

Duration:

This charter will be reviewed for resubmission in one year.


MARTA S. Q. DAVIDSON Date
Lieutenant Colonel, MSC,
Deputy PAD/HIPAA Privacy WIPT Project Officer


DAVETTE L. MURRAY Date
Lieutenant Colonel, MS
Deputy CIO /HIPAA Project Manager

AMEDD HIPAA Privacy Working Integrated Project Team Participants				
Position	Name	Phone	DSN	E-Mail Address
AMEDD HIPAA Privacy Project Manager Deputy Chief, Patient Administration Division, ACSHP&S	LTC Marta Davidson	210-221-6113	471	Marta.Davidson@amedd.army.mil
OTSG - Patient Admin Division	COL Mary Ancker	703-681-2708	761	Mary.Ancker@amedd.army.mil
OTSG - Patient Admin Division	LTC Shelia Hobbs	703-681-3113	761	Shelia.Hobbs@amedd.army.mil
Medical Records Consultant	Ms. Terry Foley	703-681-3109	761	Teresa.Foley@amedd.army.mil
PASBA Representative	MAJ Deborah Wesloh	210-295-8936	471	Deborah.Wesloh@amedd.army.mil
AC&S Representatives	MAJ Peter Marks	210-221-7337	471	Peter.Marks@amedd.army.mil
	MAJ Wanda Wade	210-221-8675	471	Wanda.Wade@amedd.army.mil
CHPPM Representative	Ms. Janet Blackburn	410-436-7222	584	Janet.Blackburn@amedd.army.mil
DENCOM Representative	COL John Storz	210-221-8241	471	John.Storz@amedd.army.mil
MRMC Representative	Ms. Phylis Rinehart	301-619-7547	343	Phylis.Rinehart@det.amedd.army.mil
ERMC Representatives	MAJ Toni Jackman	314-371-3383	--	Toni.Jackman@amedd.army.mil
	Ms. Rebecca Bridges	314-371-3188	---	Rebecca.Bridges@amedd.army.mil
GPRMC Representatives	MAJ Myron Fay	210-916-1029	471	Myron.Fay@amedd.army.mil
NARMC Representative	COL Mary Bedell	202-782-9094	662	Mary.Bedell@amedd.army.mil
PRMC Representative	CPT Jennifer Gerald	808-433-2327		Jennifer.Gerald@amedd.army.mil
SERMC Representative	MAJ Rick Clabaugh	706-787-3577	780	Rick.Clabaugh@amedd.army.mil

C-2-3

AMEDD HIPAA Privacy Working Integrated Project Team Participants				
Position	Name	Phone	DSN	E-Mail Address
WRMC Representative	LTC Michael Griffin	253-968-1795	357	Michael.Griffin2@amedd.army.mil
18 th MEDCOM Representative	MAJ Matthew Horsley	315-737-8554	780	Matthew.Horsley@amedd.army.mil
AFIP Representative	Ms. Annette Anderson	202-782-2500	662	andersona@afip.osd.mil
WIPT Recorder HIPAA Privacy Contractor Support	Mr. Tom Leonard, PEC Solutions, Inc.	210-221-7841	471	Tom.Leonard@amedd.army.mil

C-3. AMEDD HIPAA Security WIPT Charter and Member Information.**CHARTER****U.S. ARMY MEDICAL DEPARTMENT
Health Insurance Portability and Accountability Act
Security Working Integrated Project Team****Purpose**

The Health Insurance Portability and Accountability Act (HIPAA) Security Working Integrated Project Team (Security WIPT) will develop a compliance strategy and provide oversight of the execution process to ensure that all HIPAA Security requirements are implemented accurately and in a timely manner.

The HIPAA Security WIPT will support the HIPAA Overarching IPT as required and report to the HIPAA OIPT on a periodic basis.

The HIPAA Security WIPT Project Manager may task appropriate offices within the U. S. Army Medical Command and Office of the Surgeon General for various HIPAA Security requirements.

Membership

MEDCOM Information Assurance Program Manager (Project Manager for HIPAA Security WIPT) - Chairman

MEDCOM Major Subordinate Command Representatives

- Dental Command
- Veterinary Command
- Center for Health Promotion and Preventive Medicine
- AMEDD Center and School
- Medical Research and Materiel Command
- USAMISSA
- Regional Medical Commands

Additional participants may be added as needed, at the discretion of the Project Manager.

Meetings

Meetings will be held monthly during the life cycle of the program. The Project manager may adjust this schedule as required.

Deliverables

Deliverables will include the following:

- Implementation Plan and Timeline
- Compliance Strategy Plans

- Tasking Documents
- Appoint MISRT
- Pursue OCTAVE Training for Security Officers
- Security Risk Assessment
- HIPAA Security Rule Readiness Checklist
- Policy Recommendations and Guidelines
- Certification and Accreditation Recommendations
- Progress Reports

The HIPAA Security WIPT Project Managers will publish approved minutes .

Duration

This charter will be reviewed for resubmission in one year.

Effective Date

This charter becomes effective on the date it is signed by the Deputy Surgeon General.



Barziel Lee Drewry Date
HQ MEDCOM/MCIM
MEDCOM IAPM /HIPAA Security WIPT Project Officer

 14 Jun 03
DAVETTE L. MURRAY Date
Lieutenant Colonel
Deputy Chief Information Officer/HIPAA Project Manager

AMEDD HIPAA Security Working Integrated Project Team Participants				
Position	Name	Phone	DSN Prefix	E-Mail Address
AMEDD HIPAA Security WIPT Chair, Chief, Plans and Policies, Office of the Assistant Chief of Staff for Information Management	Mr. Barzie Drewry	210-221-6836	471	Barzie.Drewry@amedd.army.mil
AMEDD HIPAA Security Project Manager, Office of the Assistant Chief of Staff for Information Management	Mr. Ross Roberts	210-221-7869	471	Ross.Roberts@amedd.army.mil
AMEDDC&S Representative	Mr. Ralph Coogan	210-221-8639	471	Ralph.Coogan@amedd.army.mil
CHPPM Representative	Ms. Janet Blackburn	410-436-7222	584	Janet.Blackburn@amedd.army.mil
DENCOM Representative	TBD			
VETCOM Representative	Mr. Lafon Lively	210-221-6697	471	Lafon.Lively@amedd.army.mil
MRMC Representative	Ms. Phylis Rinehart	301-619-7547	343	Phylis.Rinehart@amedd.army.mil
ERMC Representative	Ms. Rebecca Bridges	314-371-3191 (DSN)	NA	Rebecca.Bridges@amedd.army.mil
GPRMC Representatives	Mr. William Todd	210-295-2333	421	William.Todd@amedd.army.mil
NARMC Representative	Ms. Debbie Rivers	202-782-5761	662	Debbie.Rivers@amedd.army.mil
PRMC Representative	Ms. Kathy Auxer	808-433-5033		Kathryn.auxer@amedd.army.mil
SERMC Representatives	Dr. Woody Miller	706-787-1062	773	Woodrow.Miller@amedd.army.mil
WRMC Representative	Mr. Karl Anderson	253-968-0334	782	Karl.Anderson@amedd.army.mil
USAMISSA Representative	Mr. Guy Sherburne	210-637-2493 471-9719/x2493 (DSN)	NA	Guy.Sherburne@amedd.army.mil
18 TH MEDCOM Representative	TBD			
WIPT Recorder	Ms. Jan Eagan, PEC Solutions, Inc.	210-221-8989	471	Janet.Eagan@amedd.army.mil

LIST OF FIGURES AND TABLES**Figures**

Figure 1. HIPAA Rules and Provisions	7
Figure 2. MHS HIPAA OIPT/WIPT Structure	12
Figure 3. AMEDD HIPAA OIPT/WIPT Structure	13
Figure 4. Headquarters Directorate, Executive Agency, and MSC HIPAA Implementation Team Structure	14
Figure 5. MTF/DTF HIPAA Implementation Team Structure	15

Tables

Table 1. HIPAA Compliance Dates.....	8
Table 2. TMA Privacy Initiatives	20
Table 3. AMEDD Privacy Initiatives	22
Table 4. General Privacy Tasks for Headquarters Directorates, Executive Agents, and MSCs	24
Table 5. Additional Privacy Tasks for RMCs	25
Table 6. Privacy Tasks for MTF/DTFs	26
Table 7. Key Similarities Between Privacy and Security Rules	28
Table 8. TMA Security Initiatives	30
Table 9. AMEDD Security Initiatives	32
Table 10. Comparison of HIPAA and Military Security Requirements	33
Table 11. Security Rule Implementation and Certification Timelines.....	35
Table 12. Security Tasks and Timelines for Headquarters Directorates, Executive Agencies, MSCs, MTFs, and DTFs	36

LIST OF ABBREVIATIONS AND ACRONYMS

ACSHP&S	Assistant Chief of Staff for Health Policy and Services
ACSIM	Assistant Chief of Staff for Information Management
ACSPER	Assistant Chief of Staff for Personnel
ACSRM	Assistant Chief of Staff for Resource Management
AFIP	Armed Forces Institute of Pathology
AHA	American Hospital Association
AKCC	Army Knowledge Collaboration Center
AKO	Army Knowledge Online
AMEDD	US Army Medical Department
AMEDDC&S / AC&S	US Army Medical Department Center and School
ANSI	American National Standards Institute
ASC	Accredited Standards Committee
C&A	Certification and Accreditation
CAC	Common Access Card
CCIR	Commander's Critical Information Requirement
CDT™	Current Dental Terminology
CE	Covered Entity
CHCS/ADM	Composite Health Care System/Ambulatory Data Module
CHPPM	US Army Center for Health Promotion and Preventive Medicine
CIO	Chief Information Officer
CMS	Centers for Medicare and Medicaid Services
COOP	Continuity of Operations Plan
CPS II	Claims Processing System II
CPT	Current Procedural Terminology
CSD	Clinical Services Division
CUITN	Common User Installation Transport Network
DEERS	Defense Enrollment Eligibility Reporting System
DENCOM	US Army Dental Command
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DoD	Department of Defense

DOIM.....	Directorate of Information Management
DSN	Defense Switch Network
DTF	Dental Treatment Facility
EDI	Electronic Data Interchange
EI/DS.....	Executive Information/Decision Support
EIN	Employer Identification Number
ERMC	US Army Europe Regional Medical Command
EWRAS.....	Enterprise-Wide Authorization and Referral System
FAQs.....	Frequently Asked Questions
FOIA.....	Freedom of Information Act
GPRMC.....	US Army Great Plains Regional Medical Command
HCAA	Health Care Acquisition Activity
HCFA	Health Care Financing Administration
HCPCS	Health Care Financing Administration Common Procedural Coding System
HCS	HIPAA Compliance Specialist
HHS	Health and Human Services (Department of)
HIMSS.....	Health Information Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HQ.....	Headquarters
ICD-9-CM.....	International Classification of Diseases, 9 th Revision, Clinical Modification
IAPM	Information Assurance Program Manager
IAVA.....	Information Assurance Vulnerability Alert
IAW	In Accordance With
IIHI	Individually Identifiable Health Information
IMD	Information Management Directorate
MCSC	Managed Care Support Contractor
MEDCEN	US Army Medical Center
MEDCOM.....	US Army Medical Command
MHS	Military Health System
MISRT	Medical Information Security Readiness Team
MOA.....	Memorandum of Agreement
MOU.....	Memorandum of Understanding

MRMC	US Army Medical Research and Materiel Command
MSC	Major Subordinate Command
MTF	Military Treatment Facility
NARMC	US Army North Atlantic Regional Command
NCPDP	National Council for Prescription Drug Programs
NGB	The National Guard Bureau
NOPP	Notice of Privacy Practices
NPI	National Provider Identifier
NPRM	Notice of Proposed Rulemaking
OCAR	Office of the Chief Army Reserve
OCR	Office for Civil Rights
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OIPT	Overarching Integrated Project/Product/Program Team
OTSG	Office of The Surgeon General
PAD	Patient Administration Division
PASBA	Patient Administration Systems and Biostatistics Activity
PDF	Portable Document Format
PDTS	Pharmacy Data Transaction System
PHI	Protected Health Information
PKI	Public Key Infrastructure
POC	Point of Contact
PRMC	US Army Pacific Regional Medical Command
Regs	Regulations
RIMR	Risk Information Management Resource
RMC	Regional Medical Command
SCR	System Change Request
SERMC	US Army Southeast Regional Medical Command
SJA	Staff Judge Advocate
SM	Service Mark
SMART	Standardized Materials and Research Technology
SNIP	Strategic National Implementation Process
TATRC	Telemedicine & Advanced Technology Research Center

TBD.....	To Be Determined
T&CS	Transactions and Code Sets
TIMPO.....	Tri-Service Infrastructure Management Program Office
TM.....	Trade Mark
TMA	TRICARE Management Activity
TPO.....	Treatment, Payment, and Health Care Operations
TPOCS.....	Third Party Outpatient Collection System
USARC	US Army Reserve Command
USAMISSA	US Army Medical Information Systems and Services Agency
VETCOM.....	US Army Veterinary Command
VLAN.....	Virtual Local Area Network
VPN.....	Virtual Private Network
WEDI.....	Workgroup for Electronic Data Interchange
WIPT	Working Integrated Project/Product/Program Team
WRMC	US Army Western Regional Medical Command

X12..... An American National Standards Institute (ANSI) accredited group that defines EDI standards for many American industries, including health care insurance. The HIPAA prescribes that the standards mandated under it be developed by ANSI accredited bodies whenever practical. Most of the electronic transaction standards mandated or proposed under HIPAA are X12 standards. These transactions are as follows:

- X12 270 - Health Care Eligibility & Benefit Inquiry transaction.
- X12 271- Health Care Eligibility & Benefit Response transaction.
- X12 276 - Health Care Claims Status Inquiry transaction.
- X12 277 - Health Care Claims Status Response transaction.
- X12 278 - Referral Certification and Authorization transaction.
- X12 820 - Payment Order & Remittance Advice transaction.
- X12 834 - Benefit Enrollment & Maintenance transaction.
- X12 835 - Health Care Claims Payment & Remittance Advice transaction.
- X12 837 - Health Care Claims or Encounter transaction.